UNIA EUROPEJSKA

PARLAMENT EUROPEJSKI **RADA**

Bruksela, 15 listopada 2023 r.
(OR. en)

2022/0047 (COD) **PE-CONS 49/23**

TELECOM 237
COMPET 781
MI 650
DATAPROTECT 205
JAI 1045
PI 116
CODEC 1418

AKTY USTAWODAWCZE I INNE INSTRUMENTY

Dotyczy:	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY 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)

ROZPORZĄDZENIE
PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2023/…

z dnia ...

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)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Banku Centralnego[1],

[1] Dz.U. C 402 z 19.10.2022, s. 5.

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],

uwzględniając opinię Komitetu Regionów[2],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[3],

[1] Dz.U. C 365 z 23.9.2022, s. 18.
[2] Dz.U. C 375 z 30.9.2022, s. 112.
[3] Stanowisko Parlamentu Europejskiego z dnia 9 listopada 2023 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia … r.

a także mając na uwadze, co następuje:

(1) Na przestrzeni ostatnich lat technologie oparte na danych doprowadziły do przemian we wszystkich sektorach gospodarki. W szczególności szybki wzrost liczby produktów podłączonych do internetu przyczynił się do zwiększenia ilości danych i ich potencjalnej wartości dla konsumentów, przedsiębiorstw i ogółu społeczeństwa. Wysokiej jakości interoperacyjne dane z różnych dziedzin sprzyjają konkurencyjności i innowacyjności oraz zapewniają zrównoważony wzrost gospodarczy. Te same dane mogą zostać wykorzystane i być ponownie wykorzystywane do wielu różnych celów i w nieograniczonym zakresie, bez jakiegokolwiek uszczerbku dla jakości czy ilości.

(2) Bariery utrudniające dzielenie się danymi uniemożliwiają optymalne wykorzystywanie danych z pożytkiem dla społeczeństwa. Bariery te obejmują brak czynników zachęcających posiadaczy danych do dobrowolnego zawierania umów o dzieleniu się danymi, brak pewności w kwestii praw i obowiązków związanych z danymi, koszty zawierania umów na interfejsy techniczne i wdrażania tych interfejsów, wysoki poziom rozdrobnienia informacji w silosach danych, niezadowalająca jakość zarządzania metadanymi, brak norm interoperacyjności semantycznej i technicznej, wąskie gardła utrudniające dostęp do danych, brak wspólnych praktyk w dziedzinie dzielenia się danymi oraz nadużywanie braku równowagi kontraktowej w kwestiach dotyczących dostępu do danych i ich wykorzystywania.

(3) W sektorach charakteryzujących się znacznym udziałem mikroprzedsiębiorstw, małych przedsiębiorstw i średnich przedsiębiorstw, zdefiniowanych w art. 2 załącznika do zalecenia Komisji 2003/361/WE[1] (MŚP), niejednokrotnie można zaobserwować niedobór zdolności cyfrowych oraz umiejętności zbierania, analizowania i wykorzystywania danych; ponadto dostęp do danych często jest ograniczony z uwagi na fakt, że jeden podmiot ma je w posiadaniu w swoim systemie, lub z uwagi na brak interoperacyjności między danymi, brak interoperacyjności między usługami w zakresie danych czy brak interoperacyjności transgranicznej.

(4) Aby zaspokoić potrzeby gospodarki cyfrowej i usunąć bariery stojące na drodze do dobrze prosperującego wewnętrznego rynku danych, należy ustanowić zharmonizowane ramy określające, kto jest uprawniony do wykorzystywania danych z produktu lub z usługi powiązanej, na jakich warunkach i na jakiej podstawie. Państwa członkowskie nie powinny zatem przyjmować ani utrzymywać dodatkowych wymagań krajowych w odniesieniu do kwestii wchodzących w zakres stosowania niniejszego rozporządzenia, chyba że wyraźnie stanowi ono inaczej, ponieważ miałoby to wpływ to na jego bezpośrednie i jednolite stosowanie. Ponadto działanie na poziomie Unii powinno pozostawać bez uszczerbku dla obowiązków i zobowiązań ustanowionych w międzynarodowych umowach handlowych zawartych przez Unię.

---

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

(5) Celem niniejszego rozporządzenia jest zapewnienie użytkownikom produktu skomunikowanego lub usługi powiązanej w Unii możliwości terminowego dostępu do danych generowanych w wyniku korzystania z danego produktu skomunikowanego lub z danej usługi powiązanej oraz wykorzystywania tych danych, w tym dzielenia się nimi z wybranymi przez siebie osobami trzecimi. Nakłada ono na posiadaczy danych obowiązek udostępniania danych w określonych okolicznościach użytkownikom i osobom trzecim wybranym przez użytkowników. Zapewnia również, aby posiadacze danych udostępniali dane odbiorcom danych w Unii na sprawiedliwych, rozsądnych i niedyskryminujących zasadach oraz w sposób przejrzysty. Kluczowe znaczenie w ramach dzielenia się danymi mają przepisy prawa prywatnego. Z tego względu w niniejszym rozporządzeniu dostosowuje się przepisy prawa zobowiązań i zapobiega nadużywaniu braku równowagi kontraktowej, która utrudnia sprawiedliwy dostęp do danych i ich uczciwe wykorzystywanie. W przypadku wystąpienia wyjątkowej potrzeby, niniejsze rozporządzenie nakłada również na posiadaczy danych obowiązek udostępniania organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organom Unii — danych niezbędnych do wykonywania określonego zadania realizowanego w interesie publicznym. Celem niniejszego rozporządzenia jest ponadto ułatwienie zmiany dostawcy usług przetwarzania danych, zwiększenie interoperacyjności danych oraz mechanizmów i usług dzielenia się danymi w Unii. Przepisów niniejszego rozporządzenia nie należy interpretować jako uznających ani przyznających posiadaczom danych jakiekolwiek nowe prawo do wykorzystywania danych generowanych w wyniku korzystania z produktu skomunikowanego lub usługi powiązanej.

(6) Generowanie danych stanowi rezultat działań co najmniej dwóch podmiotów, w szczególności twórców lub producentów produktu skomunikowanego, którzy w wielu przypadkach mogą być także dostawcami usług powiązanych, i użytkownika tego produktu skomunikowanego lub usług powiązanych. Rodzi to pytania o sprawiedliwość w gospodarce cyfrowej, ponieważ dane utrwalane przez takie produkty skomunikowane lub usługi powiązane są istotnymi danymi wejściowymi dla usług świadczonych na rynkach posprzedażowych, usług pomocniczych oraz innego rodzaju usług. Aby czerpać z danych znaczne korzyści gospodarcze, w tym poprzez dzielenie się danymi na podstawie dobrowolnych umów i szersze tworzenie wartości ekonomicznej na podstawie danych przez unijne przedsiębiorstwa, należy przyjąć ogólne podejście regulujące udzielanie praw dostępu do danych i ich wykorzystywania, zamiast w tym celu przyznawać prawa wyłączne. W niniejszym rozporządzeniu ustanowione są przepisy horyzontalne, a kolejnym krokiem może być ustanowienie prawa Unii lub prawa krajowego uwzględniającego konkretną sytuację stosownych sektorów.

(7) Prawo podstawowe do ochrony danych osobowych zostało zagwarantowane w szczególności w rozporządzeniach Parlamentu Europejskiego i Rady (UE) 2016/679[1] i (UE) 2018/1725[2]. Dodatkową ochronę życia prywatnego i poufności komunikacji zapewnia dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady[3], w tym poprzez określenie warunków przechowywania wszelkich danych osobowych i nieosobowych w urządzeniach końcowych oraz warunków uzyskiwania dostępu do tych danych z urządzeń końcowych. Te unijne akty prawne stanowią podstawę zrównoważonego i odpowiedzialnego przetwarzania danych, również w sytuacjach, w których zestawy danych zawierają równocześnie dane osobowe i dane nieosobowe. Niniejsze rozporządzenie uzupełnia prawo Unii w zakresie ochrony danych osobowych i prywatności, w szczególności rozporządzenia (UE) 2016/679 i (UE) 2018/1725 oraz dyrektywę 2002/58/WE, i pozostaje bez uszczerbku dla tego prawa. Żaden przepis niniejszego rozporządzenia nie powinien być stosowany ani interpretowany w sposób umniejszający lub ograniczający prawo do ochrony danych osobowych lub prawo do prywatności i poufności komunikacji.

---

1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

2 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

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

Wszelkie przetwarzanie danych osobowych zgodnie z niniejszym rozporządzeniem powinno być zgodne z prawem Unii dotyczącym ochrony danych, w tym m.in. z wymogiem istnienia ważnej podstawy prawnej do przetwarzania na podstawie art. 6 rozporządzenia (UE) 2016/679 oraz, w stosownym przypadku, z warunkami przewidzianymi w art. 9 tego rozporządzenia oraz w art. 5 ust. 3 dyrektywy 2002/58/WE. Niniejsze rozporządzenie nie stanowi podstawy prawnej do zbierania ani generowania danych osobowych przez posiadacza danych. Niniejsze rozporządzenie nakłada na posiadaczy danych obowiązek udostępniania danych osobowych użytkownikom oraz, na wniosek użytkownika, wybranym przez niego osobom trzecim. Taki dostęp powinien dotyczyć danych osobowych przetwarzanych przez posiadacza danych na mocy którejkolwiek z podstaw prawnych, o których mowa w art. 6 rozporządzenia (UE) 2016/679. W przypadku gdy użytkownik nie jest osobą, której dane dotyczą, niniejsze rozporządzenie nie stanowi podstawy prawnej do zapewniania dostępu do danych osobowych ani do ich udostępniania osobie trzeciej i nie należy go interpretować jako przyznającego posiadaczowi danych jakiekolwiek nowe prawo do wykorzystywania danych osobowych generowanych w wyniku korzystania z produktu skomunikowanego lub usługi powiązanej. W takich przypadkach w interesie użytkownika może być ułatwienie wypełnienia wymagań przewidzianych w art. 6 rozporządzenia (UE) 2016/679. Ponieważ niniejsze rozporządzenie nie powinno negatywnie wpływać na prawa do ochrony danych osobowych osób, których dane dotyczą, w takich przypadkach posiadacz danych może stosować się do wniosków m.in. przez zastosowanie anonimizacji danych osobowych lub, gdy łatwo dostępne dane zawierają dane osobowe kilku osób, których dane dotyczą, przez przekazanie wyłącznie danych osobowych dotyczących użytkownika.

(8) Zasada minimalizacji danych, uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych mają kluczowe znaczenie w sytuacji, gdy przetwarzanie danych wiąże się z istotnym ryzykiem dla praw podstawowych osób fizycznych. Biorąc pod uwagę aktualny stan wiedzy naukowej i technicznej, wszystkie strony procesu dzielenia się danymi, w tym również dzielenia się danymi w ramach zakresu stosowania niniejszego rozporządzenia, powinny wdrożyć środki techniczne i organizacyjne pozwalające na ochronę tych praw. Środki takie obejmują nie tylko pseudonimizację i szyfrowanie, lecz także korzystanie z coraz powszechniej dostępnej technologii umożliwiającej przekazywanie algorytmów do danych (ang. *bring algorithm to the data*), co pozwala wywnioskować wartościowe informacje bez konieczności przesyłania danych między stronami lub zbędnego kopiowania samych surowych lub ustrukturyzowanych danych.

(9) O ile nie zostało to odmiennie uregulowane niniejszym rozporządzeniem, niniejsze rozporządzenie nie wpływa na krajowe prawo zobowiązań, w tym na przepisy dotyczące zawierania, ważności lub skutków umów, lub konsekwencji rozwiązania umów. Niniejsze rozporządzenie uzupełnia prawo Unii mające na celu wspieranie interesów konsumentów, zapewnianie konsumentom wysokiego poziomu ochrony oraz ochronę ich zdrowia, bezpieczeństwa i interesów ekonomicznych, w szczególności dyrektywę Rady 93/13/EWG[1] oraz dyrektywy Parlamentu Europejskiego i Rady 2005/29/WE[2] i 2011/83/UE[3], i pozostaje bez uszczerbku dla tego prawa.

---

1 Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz.U. L 95 z 21.4.1993, s. 29).

2 Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady („Dyrektywa o nieuczciwych praktykach handlowych") (Dz.U. L 149 z 11.6.2005, s. 22).

3 Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz.U. L 304 z 22.11.2011, s. 64).

(10) Niniejsze rozporządzenie pozostaje bez uszczerbku dla aktów prawnych Unii i krajowych aktów prawnych ustanawiających dzielenie się danymi, dostęp do danych oraz wykorzystywanie danych do celów związanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem lub ściganiem czynów zabronionych lub wykonywaniem kar lub do celów celnych i podatkowych, niezależnie od podstawy prawnej przewidzianej w Traktacie o funkcjonowaniu Unii Europejskiej (TFUE), w oparciu o którą te unijne akty prawne zostały przyjęte, a także dla współpracy międzynarodowej w tym zakresie prowadzonej w szczególności na podstawie Konwencji Rady Europy o cyberprzestępczości sporządzonej w Budapeszcie dnia 23 listopada 2001 r. (CETS nr 185). Akty te obejmują rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784[1], (UE) 2022/2065[2], (UE) 2023/1543[3] oraz dyrektywę Parlamentu Europejskiego i Rady (UE) 2023/1544.[4]Niniejsze rozporządzenie nie ma zastosowania do gromadzenia lub udostępniania danych, dostępu do nich ani ich wykorzystywania na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/847[5] i dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849[6]. Niniejsze rozporządzenie nie ma zastosowania do dziedzin niewchodzących w zakres prawa Unii i w każdym wypadku nie wpływa na kompetencje państw członkowskich w dziedzinie bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego, administracji celnej i podatkowej lub zdrowia i bezpieczeństwa obywateli, niezależnie od rodzaju podmiotu, któremu państwo członkowskie powierzyło realizowanie zadań związanych z tymi kompetencjami.

---

1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz.U. L 172 z 17.5.2021, s. 79).

2 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. L 277 z 27.10.2022, s. 1).

3 Rozporządzenie Parlamentu Europejskiego i Rady 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L 191, 28.7.2023, s. 118).

4 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz.U. L 191, 28.7.2023, s. 181).

5 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006 (Dz.U. L 141 z 5.6.2015, s. 1).

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

(11) Niniejsze rozporządzenie nie powinno wpływać na prawo Unii określające wymagania dotyczące fizycznego projektu i wymogi dotyczące danych w przypadku produktów wprowadzanych do obrotu w Unii, chyba że niniejsze rozporządzenie wyraźnie stanowi inaczej.

(12) Niniejsze rozporządzenie jest uzupełnieniem i pozostaje bez uszczerbku dla prawa Unii określającego wymagania dostępności niektórych produktów i usług, w szczególności dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/882[1].

(13) Niniejsze rozporządzenie pozostaje bez uszczerbku dla aktów prawnych Unii i krajowych aktów prawnych przewidujących ochronę praw własności intelektualnej, w tym dyrektyw Parlamentu Europejskiego i Rady 2001/29/WE[2], 2004/48/WE[3] oraz (UE) 2019/790[4].

---

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

2 Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. L 167 z 22.6 2001, s. 10).

3 Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.U. L 157 z 30.4.2004, s. 45).

4 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.U. L 130 z 17.5.2019, s. 92).

(14) Zakres stosowania niniejszego rozporządzenia powinien obejmować produkty skomunikowane, które za pomocą elementów składowych lub systemów operacyjnych pozyskują, generują lub zbierają dane dotyczące swojego działania, wykorzystywania lub środowiska i które mogą komunikować te dane za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu, często określanych jako internet rzeczy, z wyjątkiem prototypów. Przykładem takich usług łączności elektronicznej są w szczególności naziemne sieci telefoniczne, sieci telewizji kablowej, sieci satelitarne i sieci komunikacji zbliżeniowej. Produkty skomunikowane można znaleźć we wszystkich segmentach gospodarki i życia społecznego, w tym w infrastrukturze prywatnej, cywilnej i handlowej, w pojazdach, w sprzęcie związanym ze zdrowiem i stylem życia, na statkach, w statkach powietrznych, w sprzętach domowych i towarach konsumpcyjnych, wyrobach medycznych i zdrowotnych lub maszynach rolniczych i przemysłowych. O tym, jakie dane jest w stanie udostępniać produkt skomunikowany, powinny decydować wybory projektowe producenta oraz w stosownym przypadku prawo Unii lub prawo krajowe uwzględniające potrzeby i cele danego sektora lub stosowne decyzje właściwych organów.

(15) Dane stanowią cyfrowe odwzorowanie czynności i zdarzeń z udziałem użytkownika i w związku z tym powinny być dla niego dostępne. Przepisy niniejszego rozporządzenia dotyczące dostępu do danych z produktów skomunikowanych i usług powiązanych oraz dotyczące ich wykorzystywania odnoszą się zarówno do danych z produktu, jak i do danych z usługi powiązanej. Dane z produktu to dane wygenerowane w wyniku korzystania z produktu skomunikowanego, które producent zaprojektował tak, by mogły być pobierane przez użytkownika, posiadacza danych lub osobę trzecią, w tym w stosownym przypadku producenta. Dane z usługi powiązanej to dane stanowiące cyfrowe odwzorowanie czynności lub zdarzeń z udziałem użytkownika związanych z produktem skomunikowanym, generowane podczas świadczenia usługi powiązanej przez dostawcę. Dane wygenerowane w wyniku korzystania z produktu skomunikowanego lub z usługi powiązanej należy rozumieć jako dane utrwalone celowo lub dane niebezpośrednio wynikające z czynności użytkownika, takie jak dane o środowisku produktu skomunikowanego lub o jego interakcjach. Powinny one obejmować dane o korzystaniu z produktu skomunikowanego wygenerowane przez interfejs użytkownika lub poprzez usługę powiązaną i nie powinny ograniczać się do informacji, że takie korzystanie miało miejsce, lecz powinny obejmować wszelkie dane, które generuje produkt skomunikowany w wyniku takiego korzystania, takie jak dane wygenerowane automatycznie przez czujniki oraz dane utrwalone przez wbudowane aplikacje, w tym aplikacje wskazujące stan i nieprawidłowe działanie urządzenia. Powinny one także obejmować dane wygenerowane przez produkt skomunikowany lub usługę powiązaną podczas bezczynności użytkownika, np. gdy użytkownik postanawia nie korzystać z produktu skomunikowanego przez określony czas i pozostawić go w trybie czuwania lub nawet go wyłączyć, z uwagi na to, że stan produktu skomunikowanego lub jego elementów składowych, takich jak baterie, może się różnić, gdy produkt skomunikowany znajduje się w trybie czuwania lub jest wyłączony. W zakres stosowania niniejszego rozporządzenia wchodzą dane, które nie są w znaczny sposób zmodyfikowane, tzn. dane surowe, nazywane także danymi źródłowymi czy danymi pierwotnymi, oznaczające punkty danych automatycznie generowane bez dalszego przetwarzania oraz dane, które zostały wstępnie przetworzone, po to aby przed dalszym przetwarzaniem i analizą były zrozumiałe i użyteczne.

Takie dane obejmują dane zebrane przez pojedynczy czujnik lub przez skomunikowaną grupę czujników do celów uczynienia zebranych danych zrozumiałymi na potrzeby ich szerszego wykorzystania, poprzez określenie wielkości lub właściwości fizycznej lub zmiany wielkości fizycznej, np. temperatury, ciśnienia, natężenia przepływu, dźwięku, wartości pH, poziomu cieczy, pozycji, przyspieszenia lub prędkości. Terminu „dane wstępnie przetworzone” nie należy interpretować w sposób nakładający na posiadacza danych obowiązku dokonywania znacznych inwestycji w czyszczenie i transformację danych. Dane, które mają być udostępnione, powinny obejmować stosowne metadane, w tym ich podstawowy kontekst i znacznik czasu, aby dane były użyteczne w połączeniu z innymi danymi, takimi jak dane posortowane i sklasyfikowane z innymi odnoszącymi się do nich punktami danych, lub przeformatowane na powszechnie używany format. Takie dane mogą być cenne dla użytkownika i przyczyniać się do innowacji i do opracowania usług cyfrowych i innych usług chroniących środowisko, zdrowie i gospodarkę o obiegu zamkniętym, w tym poprzez umożliwianie konserwacji i naprawy przedmiotowych produktów skomunikowanych. W zakres niniejszego rozporządzenia nie powinny jednak wchodzić informacje wywiedzione lub wywnioskowane z takich danych a które są wynikiem dodatkowych inwestycji w przypisywanie wartości do danych lub pozyskiwanie wiedzy z danych, w szczególności za pomocą złożonych algorytmów autorskich, w tym będących częścią oprogramowania zamkniętego, i w związku z tym obowiązek udostępniania tych informacji użytkownikowi lub odbiorcy danych spoczywający na posiadaczu danych nie powinien ich obejmować, chyba że użytkownik i posiadacz danych wspólnie postanowią inaczej. Dane takie mogą obejmować w szczególności informacje wywnioskowane za pomocą fuzji sensorycznej, która wywodzi lub wywnioskowuje dane z wielu czujników zebranych w produkcie skomunikowanym przy użyciu złożonych algorytmów autorskich i która może podlegać prawom własności intelektualnej.

(16) Niniejsze rozporządzenie pozwala użytkownikom produktów skomunikowanych korzystać z usług świadczonych na rynkach posprzedażowych, z usług pomocniczych oraz z innego rodzaju usług opartych na danych zebranych przez czujniki wbudowane w takie produkty; zbieranie tych danych może być wartościowe dla poprawy działania produktów skomunikowanych. Ważne jest, aby rozróżnić z jednej strony rynki oferujące takie wyposażone w czujniki produkty skomunikowane oraz usługi powiązane, a z drugiej – rynki niepowiązanego oprogramowania i niepowiązanych treści, takich jak treści tekstowe, dźwiękowe lub audiowizualne, często objęte prawami własności intelektualnej. W związku z tym zakresem stosowania niniejszego rozporządzenia nie powinny być objęte dane generowane przez takie wyposażone w czujniki produkty skomunikowane, gdy użytkownik utrwala, przesyła, wyświetla lub odtwarza treści, oraz same treści, często objęte prawami własności intelektualnej, w tym na użytek usługi online. Niniejsze rozporządzenie nie powinno również obejmować danych pozyskiwanych, generowanych lub dostępnych z produktu skomunikowanego lub na niego przesyłanych do celów przechowywania lub innych operacji przetwarzania w imieniu innych osób niebędących użytkownikami, tak jak może to mieć miejsce w przypadku serwerów lub infrastruktury chmury obsługiwanych przez właścicieli wyłącznie w imieniu osób trzecich, w tym na użytek usługi online.

(17) Należy ustanowić zasady dotyczące produktów, które podczas zakupu, najmu, dzierżawy lub leasingu są skomunikowane z usługą powiązaną w taki sposób, że jej brak uniemożliwiłby produktowi skomunikowanemu wykonywanie co najmniej jednej z jego funkcji, lub która później zostaje skomunikowana z produktem przez producenta lub osobę trzecią, aby dodać lub zmodyfikować funkcje produktu skomunikowanego. Takie usługi powiązane obejmują wymianę danych między produktem skomunikowanym a dostawcą usługi i należy je rozumieć jako ściśle powiązane z obsługą funkcji produktu skomunikowanego, takie jak usługi, które w stosownym przypadku przesyłają polecenia do produktu skomunikowanego, które są w stanie mieć wpływ na jego czynności lub działanie. Usługi, które nie wpływają na obsługę produktu skomunikowanego i które nie obejmują przesyłania danych ani poleceń do produktu skomunikowanego przez dostawcę usługi, nie powinny być uznawane za usługi powiązane. Wśród usług takich mogą być konsultacje pomocnicze, usługi analityczne lub finansowe czy też bieżąca naprawa i konserwacja. Usługi powiązane mogą być oferowane w ramach umowy sprzedaży, najmu, dzierżawy czy leasingu. Usługi powiązane mogą też być świadczone w przypadku produktów tego samego rodzaju, a zatem użytkownicy mogą się spodziewać ich świadczenia uwzględniając charakter produktu i wszelkie publiczne oświadczenia ze strony lub w imieniu sprzedawcy, wynajmującego, wydzierżawiającego, leasingodawcy lub innej osoby na wcześniejszych etapach łańcucha transakcji, w tym producenta. Takie usługi powiązane mogą samodzielnie generować dane mające wartość dla użytkownika niezależnie od możliwości zbierania danych przez produkt skomunikowany, z którym są połączone. Niniejsze rozporządzenie powinno również mieć zastosowanie do usługi powiązanej dostarczanej nie przez sprzedawcę, wynajmującego, wydzierżawiającego lub leasingodawcę, lecz świadczonej przez osobę trzecią. W razie wątpliwości, czy dana usługa jest świadczona w ramach umowy sprzedaży, najmu, dzierżawy lub leasingu, niniejsze rozporządzenie powinno mieć zastosowanie. Zasilanie energią lub zapewnianie łączności nie powinny być interpretowane jako usługi powiązane do celów niniejszego rozporządzenia.

(18) Przez użytkownika produktu skomunikowanego należy rozumieć osobę fizyczną lub prawną taką jak przedsiębiorstwo, konsument lub organ sektora publicznego, do której należy produkt skomunikowany, lub która na mocy umowy najmu, dzierżawy lub leasingu otrzymała pewne prawa tymczasowe umożliwiające dostęp do danych pozyskanych z produktu skomunikowanego lub ich wykorzystywanie, lub która korzysta z usług powiązanych z produktem skomunikowanym. Prawa dostępu nie powinny w żaden sposób zmieniać ani ingerować w prawa osób, których dane dotyczą i które mogą wchodzić w interakcje z produktem skomunikowanym lub usługą powiązaną w odniesieniu do danych osobowych generowanych przez produkt skomunikowany lub podczas świadczenia usługi powiązanej. Użytkownik ponosi ryzyko i czerpie korzyści w związku z korzystaniem z produktu skomunikowanego i powinien mieć również dostęp do danych generowanych przez ten produkt. Użytkownik powinien być zatem również uprawniony do czerpania korzyści związanych z danymi generowanymi przez ten produkt skomunikowany i każdą usługę powiązaną. Za użytkownika należy również uznać właściciela, najemcę, dzierżawcę lub leasingobiorcę, w tym gdy za użytkowników można uznać kilka podmiotów. W przypadku kilku użytkowników każdy z nich może w różny sposób przyczyniać się do generowania danych i być zainteresowany różnymi formami ich wykorzystywania, tak jak ma to miejsce między innymi przy zarządzaniu flotą przedsiębiorstwa leasingowego czy w ramach rozwiązań mobilnościowych dla osób fizycznych korzystających z usługi wspólnego użytkowania samochodów osobowych.

(19) Umiejętność korzystania z danych oznacza umiejętności, wiedzę i zrozumienie, które pozwalają użytkownikom, konsumentom i przedsiębiorstwom, w szczególności MŚP objętym zakresem stosowania niniejszego rozporządzenia, zdawać sobie sprawę z potencjalnej wartości danych, które generują, które tworzą i którymi się dzielą, oraz być zmotywowanymi, by oferować i zapewniać dostęp zgodnie ze stosownymi przepisami prawnymi. Umiejętność korzystania z danych powinna wykraczać poza uczenie się o narzędziach i technologiach i powinna służyć zdobywaniu przez obywateli i przedsiębiorstwa zdolności i potencjału korzystania z inkluzywnego i uczciwego rynku danych. Rozpowszechnienie środków rozwijających umiejętność korzystania z danych oraz wprowadzenie odpowiednich działań następczych mogłyby przyczynić się do poprawy warunków pracy, a w ostatecznym rozrachunku wsparłyby konsolidację i innowacyjną ścieżkę gospodarki opartej na danych w Unii. Właściwe organy powinny promować narzędzia i przyjmować środki zwiększające wśród użytkowników i podmiotów objętych zakresem niniejszego rozporządzenia umiejętność korzystania z danych oraz świadomość przysługujących im na jego podstawie praw i spoczywających na nich obowiązków.

(20) W praktyce nie wszystkie dane generowane przez produkty skomunikowane lub usługi powiązane są łatwo dostępne dla użytkowników, a możliwość przenoszenia danych generowanych przez produkty podłączone do internetu często jest ograniczona. Użytkownicy nie są w stanie pozyskiwać danych niezbędnych do korzystania z usług naprawy i innych usług oferowanych przez dostawców, a przedsiębiorstwa nie są w stanie wprowadzać innowacyjnych, wygodnych i wydajniejszych usług. W wielu sektorach na podstawie kontroli technicznego projektu produktów skomunikowanych lub usług powiązanych producenci są w stanie ustalić, jakie dane są generowane i w jaki sposób można uzyskać do nich dostęp, mimo że nie mają tytułu prawnego do tych danych. Należy zatem zapewnić, aby produkty skomunikowane były projektowane i wytwarzane, a usługi powiązane projektowane i świadczone, w taki sposób, aby użytkownik zawsze mógł z łatwością i bezpiecznie uzyskać dostęp do danych z produktu i usługi powiązanej, w tym powiązanych metadanych niezbędnych do interpretacji i wykorzystania tych danych, w tym w celu ich pobierania i wykorzystywania oraz dzielenia się nimi – nieodpłatnie, w całościowym, ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Dane z produktu i dane z usługi powiązanej, które posiadacz danych zgodnie z prawem pozyskuje lub może zgodnie z prawem pozyskać z produktu skomunikowanego lub z powiązanej usługi, w tym dzięki projektowi produktu skomunikowanego, umowie posiadacza danych z użytkownikiem na świadczenie usług powiązanych oraz dzięki technicznym metodom dostępu do danych, bez nieproporcjonalnego wysiłku, są nazywane „danymi łatwo dostępnymi”. Dane łatwo dostępne nie obejmują danych generowanych w wyniku korzystania z produktu skomunikowanego, jeżeli projekt produktu skomunikowanego nie przewiduje przechowywania lub przesyłania takich danych poza elementem składowym, w którym są one generowane, lub poza całym produktem.

Nie należy zatem rozumieć, że niniejsze rozporządzenie wprowadza obowiązek przechowywania danych na centralnej jednostce obliczeniowej produktu skomunikowanego. Brak takiego obowiązku nie powinien uniemożliwiać producentowi lub posiadaczowi danych dokonywania dobrowolnych uzgodnień z użytkownikiem w sprawie wprowadzenia takich adaptacji. Przewidziane w niniejszym rozporządzeniu obowiązki związane z projektem pozostają także bez uszczerbku dla zasady minimalizacji danych określonej w art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679 i nie należy ich rozumieć jako wprowadzających obowiązek projektowania produktów skomunikowanych i usług powiązanych w taki sposób, aby przechowywały lub w inny sposób przetwarzały dane osobowe inne niż dane osobowe niezbędne do celów, w których są przetwarzane. Prawo Unii lub prawo krajowe może zostać ustanowione w celu doprecyzowania dalszej specyfiki, takiej jak dane z produktu, które powinny być dostępne z produktów skomunikowanych lub usług powiązanych, ponieważ takie dane mogą być nieodzowne do skutecznej obsługi, naprawy lub konserwacji tych produktów skomunikowanych lub usług powiązanych. W przypadku gdy późniejsze aktualizacje lub przeróbki produktu skomunikowanego lub usługi powiązanej przez producenta lub inną osobę skutkują dodatkowymi dostępnymi danymi lub ograniczeniem pierwotnie dostępnych danych, o zmianach takich powinno się poinformować użytkownika w kontekście aktualizacji lub przeróbki.

(21) W przypadku gdy za użytkowników uznawanych jest kilka osób lub podmiotów, np. w razie współwłasności lub w razie gdy właściciel, najemca, dzierżawca lub leasingobiorca współdzielą prawa dostępu do danych lub ich wykorzystywania, projekt produktu skomunikowanego, usługi powiązanej lub stosownego interfejsu powinien umożliwiać każdemu z użytkowników dostęp do generowanych przez niego danych. Użytkownicy produktów skomunikowanych zwykle muszą założyć konto użytkownika. Takie konto umożliwia identyfikację użytkownika przez posiadacza danych, który może być producentem. Może być również wykorzystywane jako środek komunikacji oraz do składania i przetwarzania wniosków o dostęp do danych. W przypadku gdy kilku producentów lub dostawców usług powiązanych sprzedało, wynajęło, wydzierżawiło lub oddało w leasing produkty skomunikowane lub świadczyło usługi powiązane, które są wspólnie zintegrowane, temu samemu użytkownikowi, użytkownik ten powinien zwrócić się do każdej ze stron, z którą zawarł umowę. Producenci lub projektanci produktu skomunikowanego, z którego zwykle korzysta kilka osób, powinni zapewnić niezbędne mechanizmy w stosownym przypadku umożliwiające założenie oddzielnych kont użytkownika dla poszczególnych osób lub korzystanie z tego samego konta użytkownika przez kilka osób. Rozwiązania dotyczące konta powinny pozwalać użytkownikom usuwać konta i związane z nimi dane i mogą pozwalać użytkownikom zakończyć dostęp do danych, ich wykorzystywanie lub dzielenie się nimi lub składać wnioski o takie zakończenie, w szczególności z uwzględnieniem sytuacji, w których zmienia się właściciel produktu skomunikowanego lub sposób jego użytkowania. Użytkownik powinien uzyskiwać dostęp za pomocą zwykłych mechanizmów, które automatycznie wykonują wniosek, bez konieczności analizy lub zatwierdzenia ze strony producenta lub posiadacza danych. Oznacza to, że dane powinny być udostępniane wyłącznie na faktyczne życzenie użytkownika. W przypadku gdy automatyczne wykonanie wniosku o dostęp do danych jest niemożliwe np. za pomocą konta użytkownika lub aplikacji mobilnej towarzyszącej produktowi skomunikowanemu lub usłudze powiązanej, producent powinien poinformować użytkownika, w jaki sposób może on uzyskać dostęp do danych.

(22) Produkty skomunikowane mogą być zaprojektowane tak, aby niektóre dane były bezpośrednio dostępne w pamięci urządzenia lub na zdalnym serwerze, któremu dane są komunikowane. Dostęp do pamięci urządzenia można zapewnić za pomocą kablowych lub bezprzewodowych sieci lokalnych podłączonych do publicznie dostępnych usług łączności elektronicznej lub do sieci mobilnej. Serwerem może być własny lokalny serwer producenta lub serwer osoby trzeciej lub dostawcy usług w chmurze. Podmioty przetwarzające dane zdefiniowane w art. 4 pkt 8) rozporządzenia (UE) 2016/679 nie są uznawane za posiadaczy danych. Jednakże, może być im wyznaczone konkretne zadanie udostępniania danych przez administratora danych zdefiniowane w art. 4 pkt 7) rozporządzenia (UE) 2016/679. Produkty skomunikowane mogą być zaprojektowane tak, aby użytkownik lub osoba trzecia mogli przetwarzać dane w produkcie skomunikowanym, w jednostce obliczeniowej producenta lub w wybranym przez użytkownika lub osobę trzecią środowisku informatycznym.

(23) Coraz większą rolę w ramach cyfryzacji otoczenia konsumenckiego i zawodowego odgrywają wirtualni asystenci, którzy służą jako łatwy w użyciu interfejs do odtwarzania treści, pozyskiwania informacji lub uruchamiania produktów podłączonych do internetu. Wirtualni asystenci mogą pełnić rolę pojedynczego punktu dostępu, np. w środowisku inteligentnego domu, i utrwalać znaczne ilości istotnych danych o sposobie interakcji użytkowników z produktami podłączonymi do internetu, w tym produktami wyprodukowanymi przez inne podmioty, i mogą zastępować interfejsy zapewniane przez producenta, takie jak ekrany dotykowe czy aplikacje na smartfon. Użytkownik może chcieć udostępniać takie dane zewnętrznym producentom i umożliwiać powstawanie nowatorskich inteligentnych usług. Wirtualni asystenci powinni być objęci prawami dostępu do danych przewidzianymi w niniejszym rozporządzeniu. Powinny być nimi też objęte dane generowane w trakcie interakcji użytkownika z produktem skomunikowanym za pomocą wirtualnego asystenta zapewnionego przez podmiot niebędący producentem produktu skomunikowanego. W zakres stosowania niniejszego rozporządzenia powinny wchodzić jednak wyłącznie dane wynikające z interakcji między użytkownikiem a produktem skomunikowanym lub usługą powiązaną za pośrednictwem wirtualnego asystenta. W zakres stosowania niniejszego rozporządzenia nie wchodzą dane generowane przez wirtualnego asystenta, które nie są związane z korzystaniem z produktu skomunikowanego lub usługi powiązanej.

(24) Przed zawarciem umowy sprzedaży, najmu, dzierżawy lub leasingu produktu skomunikowanego użytkownik musi otrzymać od sprzedawcy, wynajmującego, wydzierżawiającego lub leasingodawcy, którymi może być producent, jasne i zrozumiałe informacje o danych z produktu, które produkt skomunikowany jest w stanie wygenerować, w tym o rodzaju, formacie i szacowanej ilości takich danych. Może to obejmować, o ile są dostępne, informacje o strukturach danych, formatach danych, słownikach, systemach klasyfikacji, taksonomiach i wykazach kodów oraz jasne i wystarczające informacje, które są istotne dla wykonywania przez użytkownika przysługujących mu praw, o tym, jak można przechowywać dane, pobierać je lub uzyskiwać do nich dostęp, w tym warunki użytkowania i jakość usług interfejsów programowania aplikacji lub w stosownym przypadku warunki dostarczenia narzędzi dodo programowania. Obowiązek ten zapewnia przejrzystość danych generowanych z produktu i ułatwia użytkownikowi dostęp. Obowiązek informacyjny można wypełnić dzięki utrzymywaniu stabilnego ujednoliconego formatu adresowania zasobów (URL) w internecie, który można rozpowszechniać jako link do strony lub kod QR odsyłający do stosownych informacji i który może zostać wskazany użytkownikowi przez sprzedawcę, wynajmującego, wydzierżawiającego lub leasingodawcę, którymi może być producent, przed zawarciem umowy sprzedaży, najmu, dzierżawy lub leasingu produktu skomunikowanego. W każdym wypadku należy zapewnić użytkownikowi możliwość przechowywania tych informacji w sposób pozwalający na dostęp do nich w przyszłości i na odtworzenie przechowywanych informacji w niezmienionej postaci. Nie można oczekiwać, że posiadacz danych będzie bezterminowo przechowywać dane na potrzeby użytkownika produktu skomunikowanego, powinien on jednak wdrożyć rozsądną politykę zatrzymywania danych, tam, gdzie ma to zastosowanie, zgodnie z zasadą ograniczenia przechowywania zgodnie z art. 5 ust. 1 lit. e) rozporządzenia (UE) 2016/679, która pozwoli na skuteczne stosowanie praw dostępu do danych przewidzianych w niniejszym rozporządzeniu. Ten obowiązek przedstawienia informacji nie wpływa na spoczywający na administratorze danych obowiązek przedstawienia informacji osobie, której dane dotyczą, zgodnie z art. 12, 13 i 14 rozporządzenia (UE) 2016/679**.** Obowiązek przedstawienia informacji przed zawarciem umowy o świadczenie usługi powiązanej powinien spoczywać na przyszłym posiadaczu danych, niezależnie od tego, czy zawiera on umowę sprzedaży, najmu, dzierżawy lub leasingu produktu skomunikowanego. Użytkownika należy także poinformować, jeżeli w okresie trwałości produktu skomunikowanego lub w okresie obowiązywania umowy na usługę powiązaną informacje te się zmienią, w tym gdy cel, w którym dane mają być wykorzystywane, zmieni się w stosunku do celu określonego pierwotnie.

(25) Przepisów niniejszego rozporządzenia nie należy rozumieć jako przyznających posiadaczom danych jakiekolwiek nowe prawo do wykorzystywania danych z produktu lub z usługi powiązanej. W przypadku gdy posiadaczem danych jest producent produktu skomunikowanego, podstawą wykorzystywania przez niego danych nieosobowych powinna być umowa między producentem a użytkownikiem. Taka umowa może być częścią umowy o świadczenie usługi powiązanej, którą można zaoferować wraz z umową sprzedaży, najmu, dzierżawy lub leasingu dotyczącą produktu skomunikowanego. Każde postanowienie umowne stanowiące, że posiadacz danych może wykorzystywać dane z produktu lub z usługi powiązanej, powinno być dla użytkownika przejrzyste, w tym w odniesieniu do celów, w których posiadacz danych zamierza wykorzystywać dane. Cele takie mogą obejmować poprawę funkcjonowania produktu skomunikowanego lub usług powiązanych, opracowanie nowych produktów lub usług lub agregację danych w celu udostępnienia wywnioskowanych danych osobom trzecim, o ile takie wywnioskowane dane nie umożliwiają identyfikacji konkretnych danych przesłanych posiadaczowi danych z produktu skomunikowanego ani nie umożliwiają osobie trzeciej wywnioskowania tych danych z zestawu danych. Wszelkie zmiany w umowie powinny zależeć od świadomej zgody użytkownika. Niniejsze rozporządzenie nie uniemożliwia stronom uzgodnienia postanowień umownych skutkujących wykluczeniem lub ograniczeniem wykorzystywania danych nieosobowych lub niektórych kategorii danych nieosobowych przez posiadacza danych. Nie uniemożliwia ono także stronom udostępnienia – bezpośrednio lub pośrednio, albo w stosownym przypadku za pośrednictwem innego posiadacza danych, –danych z produktu skomunikowanego lub z usługi powiązanej osobom trzecim.
Co więcej, niniejsze rozporządzenie nie uniemożliwia przyjmowania sektorowych wymagań regulacyjnych w prawie Unii lub w prawie krajowym przyjętym zgodnie z prawem Unii, które to wymogi powodowałyby wykluczenie lub ograniczenie wykorzystywania niektórych takich danych przez posiadacza danych w przypadkach uzasadnionych wyraźnie zdefiniowanymi względami porządku publicznego. Niniejsze rozporządzenie nie uniemożliwia użytkownikom, w przypadku stosunków między przedsiębiorcami, udostępniania danych osobom trzecim lub posiadaczom danych na podstawie zgodnych z prawem postanowień umownych, w tym poprzez uzgodnienie ograniczenia lub zawężenia dalszego dzielenia się takimi danymi; nie uniemożliwia im także otrzymania proporcjonalnej rekompensaty, np. w zamian za zrzeczenie się prawa do wykorzystywania takich danych lub dzielenia się nimi. Pojęcie „posiadacz danych” zasadniczo nie obejmuje organów sektora publicznego, może jednak obejmować przedsiębiorstwa publiczne.

(26) Aby sprzyjać powstawaniu płynnych, uczciwych i wydajnych rynków danych nieosobowych, użytkownicy produktów skomunikowanych powinni mieć możliwość dzielenia się danymi z innymi, w tym do celów komercyjnych, przy minimalnym wysiłku prawnym i technicznym. Obecnie przedsiębiorcom często trudno jest uzasadnić koszty zatrudnienia i koszty oprogramowania, które są niezbędne do przygotowania zestawów danych nieosobowych lub produktów opartych na danych, i zaoferować je potencjalnym kontrahentom za pośrednictwem usług pośrednictwa danych, w tym rynków danych. Istotną przeszkodą w dzieleniu się danymi nieosobowymi przez przedsiębiorców jest zatem brak przewidywalności zwrotu z inwestycji w selekcję i udostępnianie zestawów danych i produktów opartych na danych. Aby umożliwić powstanie płynnych, uczciwych i wydajnych rynków danych nieosobowych w Unii, należy wyraźnie określić, która strona ma prawo oferować takie dane na rynku. Użytkownicy powinni więc mieć prawo do dzielenia się danymi nieosobowymi z odbiorcami danych w celach komercyjnych i niekomercyjnych. Takie dzielenie się danymi może być dokonywane bezpośrednio przez użytkownika, na wniosek użytkownika, za pośrednictwem posiadacza danych lub poprzez usługi pośrednictwa danych. Usługi pośrednictwa danych, regulowane rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/868[1], mogą ułatwić stworzenie gospodarki opartej na danych poprzez ustanowienie stosunków handlowych między użytkownikami, odbiorcami danych i osobami trzecimi oraz mogą wspierać użytkowników w wykonywaniu prawa do wykorzystywania danych, np. poprzez zapewnienie anonimizacji danych lub agregacji dostępu do danych osobowych pochodzących od wielu użytkowników indywidualnych. W przypadku gdy dane nie są objęte spoczywającym na posiadaczu danych obowiązku udostępniania danych użytkownikom lub osobom trzecim, zakres takich danych może zostać określony w umowie o świadczenie usługi powiązanej między użytkownikiem a posiadaczem danych, tak aby użytkownicy mogli łatwo stwierdzić, którymi danymi mogą się dzielić z odbiorcami danych lub osobami trzecimi. Posiadacze danych nie powinni udostępniać danych nieosobowych z produktu osobom trzecim w celach komercyjnych lub niekomercyjnych innych niż realizacja umowy z użytkownikiem, bez uszczerbku dla wymagań prawnych zgodnie z prawem Unii lub prawem krajowym zobowiązujących posiadacza danych do udostępniania danych. W stosownym przypadku posiadacze danych powinni umownie zobowiązać osoby trzecie, by nie dzieliły się dalej otrzymanymi od nich danymi.

---

[1] 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) (Dz.U. L 152 z 3.6.2022, s. 1).

(27) W sektorach charakteryzujących się koncentracją małej liczby producentów zaopatrujących użytkowników końcowych w produkty skomunikowane użytkownicy mogą mieć ograniczone możliwości dostępu do danych, ich wykorzystywania i dzielenia się nimi. W takich okolicznościach umowy mogą nie wystarczyć do osiągnięcia celu, którym jest wzmocnienie pozycji użytkownika, tym samym utrudniając użytkownikom czerpanie korzyści z wartości danych generowanych przez produkt skomunikowany, który kupili, wzięli w najem, w dzierżawę lub w leasing. W rezultacie innowacyjne mniejsze przedsiębiorstwa mają ograniczoną możliwość oferowania rozwiązań opartych na danych w sposób konkurencyjny i ograniczona jest możliwość rozwoju w Unii zróżnicowanej gospodarki opartej na danych. W niniejszym rozporządzeniu należy zatem oprzeć się na ostatnich dokonaniach w konkretnych sektorach, np. kodeksie postępowania w zakresie dzielenia się danymi dotyczącymi rolnictwa na podstawie umowy. Można ustanowić prawo Unii lub prawo krajowe służące zaspokojeniu potrzeb sektorowych i osiągnięciu celów sektorowych. Ponadto posiadacze danych nie powinni wykorzystywać dostępnych danych, które nie są danymi nieosobowymi, do pozyskiwania informacji o sytuacji ekonomicznej użytkownika, jego aktywach lub metodach produkcji lub o takim wykorzystywaniu przez użytkownika w żaden inny sposób, który mógłby osłabić pozycję handlową tego użytkownika na rynkach jego działalności. Może to dotyczyć wykorzystywania ze szkodą dla użytkownika wiedzy o ogólnych wynikach działalności gospodarczej lub gospodarstwa rolnego w prowadzonych z użytkownikiem negocjacjach umownych w sprawie potencjalnego nabycia produktów lub produktów rolnych użytkownika lub wprowadzania takich informacji do większych baz danych dotyczących określonych rynków w ramach danych zagregowanych, np. baz danych o wydajności plonów w nadchodzącej porze zbiorów, gdyż takie wykorzystywanie danych może pośrednio negatywnie wpłynąć na użytkownika. Użytkownik powinien otrzymać niezbędny interfejs techniczny do zarządzania zgodami, przy czym najlepiej, aby taki interfejs zawierał opcje szczegółowej kontroli zgód, np. „zezwól tylko raz” lub „zezwól podczas używania aplikacji lub usługi”, oraz możliwość cofnięcia takich zgód.

(28) W umowach między posiadaczem danych a konsumentem będącym użytkownikiem produktu skomunikowanego lub usługi powiązanej generującymi dane zastosowanie ma unijne prawo ochrony konsumentów, w szczególności dyrektywy 93/13/EWG i 2005/29/WE, które ma zapewnić, aby konsument nie podlegał nieuczciwym postanowieniom umownym. Na potrzeby niniejszego rozporządzenia nieuczciwe postanowienia umowne nałożone jednostronnie na przedsiębiorstwo nie powinny być dla tego przedsiębiorstwa wiążące.

(29) Posiadacze danych mogą wymagać odpowiedniej identyfikacji użytkownika potrzebnej do zweryfikowania, czy użytkownik jest uprawniony do uzyskania dostępu do danych. W przypadku danych osobowych przetwarzanych przez podmiot przetwarzający w imieniu administratora danych posiadacze danych powinni zapewnić, aby podmiot przetwarzający otrzymał i rozpatrzył wniosek o dostęp.

(30) Użytkownik powinien móc wykorzystywać dane w każdym zgodnym z prawem celu. Obejmuje to dostarczenie danych, które użytkownik otrzymał w ramach wykonywania praw przysługujących mu na podstawie niniejszego rozporządzenia, osobie trzeciej oferującej usługę na rynkach posprzedażowych, która może być usługą konkurencyjną względem usługi świadczonej przez posiadacza danych, lub też zlecenie takiego dostarczenia danych posiadaczowi danych. Wniosek powinien zostać złożony przez użytkownika lub przez upoważnioną osobę trzecią działającą w imieniu użytkownika, w tym dostawcę usługi pośrednictwa danych. Posiadacze danych powinni zapewnić, aby dane udostępniane osobie trzeciej były tak samo prawidłowe, kompletne, wiarygodne, stosowne i aktualne jak dane generowane w wyniku korzystania z produktu skomunikowanego lub z usługi powiązanej, do których danych posiadacz danych sam może uzyskać dostęp lub jest uprawniony do uzyskania dostępu. W ramach posługiwania się danymi należy przestrzegać wszelkich praw własności intelektualnej. Istotnym jest zachowanie zachęt do inwestowania w produkty posiadające funkcje oparte na wykorzystywaniu danych pochodzących z czujników, w które wyposażone są te produkty.

(31) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943[1] przewiduje, że pozyskiwanie, wykorzystywanie lub ujawnianie tajemnicy przedsiębiorstwa uznaje się za zgodne z prawem m.in wtedy, gdy takiego pozyskiwania, wykorzystywania lub ujawniania wymagają prawo Unii lub prawo krajowe lub gdy na nie zezwalają. Choć niniejsze rozporządzenie wymaga od posiadaczy danych ujawniania pewnych danych użytkownikom lub wybranym przez użytkownika osobom trzecim, nawet jeżeli dane te kwalifikują się do ochrony jako tajemnice przedsiębiorstwa, rozporządzenie to należy interpretować w taki sposób, aby zachować ochronę przewidzianą dla tajemnic przedsiębiorstwa na podstawie dyrektywy (UE) 2016/943. W tym kontekście posiadacze danych powinni móc wymagać od użytkowników lub wybranych przez użytkownika osób trzecich zachowania poufności danych uznawanych za tajemnice przedsiębiorstwa. W tym celu posiadacze danych powinni zidentyfikować tajemnice przedsiębiorstwa przed ujawnieniem danych i powinni móc uzgodnić z użytkownikami lub wybranymi przez użytkownika osobami trzecimi niezbędne środki służące zachowaniu poufności, w tym przez zastosowanie modelowych postanowień umownych, umów o poufności, rygorystycznych protokołów dostępu, norm technicznych oraz kodeksów postępowania. Poza posługiwaniem się modelowymi postanowieniami umownymi, które zostaną opracowane i będą zalecane przez Komisję, ustanowienie kodeksów postępowania i norm technicznych związanych z ochroną tajemnic przedsiębiorstwa w posługiwaniu się danymi może pomóc w osiągnięciu celu niniejszego rozporządzenia i powinno być promowane. W przypadku braku umowy w zakresie niezbędnych środków lub w przypadku gdy użytkownik lub wybrana przez użytkownika osoba trzecia nie stosują uzgodnionych środków lub naruszają poufność tajemnic przedsiębiorstwa, posiadacz danych powinien móc cofnąć lub zawiesić dzielenie się danymi zidentyfikowanymi jako tajemnice przedsiębiorstwa.

---

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

W takich przypadkach posiadacz danych powinien przedstawić decyzję na piśmie użytkownikowi lub osobie trzeciej bez zbędnej zwłoki i powiadomić właściwy organ państwa członkowskiego, w którym posiadacz danych ma siedzibę, że cofnął lub zawiesił dzielenie się danymi, i wskazać, których środków nie uzgodniono lub nie zastosowano oraz, w stosownym przypadku, poufność których tajemnic przedsiębiorstwa naruszono. Posiadacze danych co do zasady nie mogą odrzucić wniosku o dostęp do danych wystosowanego na podstawie niniejszego rozporządzenia wyłącznie ze względu na to, że niektóre dane uznaje się za tajemnicę przedsiębiorstwa, ponieważ przeczyłoby to zamierzonym celom niniejszego rozporządzenia. Jednak w wyjątkowych okolicznościach posiadacz danych będący posiadaczem tajemnicy przedsiębiorstwa powinien móc w indywidualnym przypadku odrzucić wniosek o dostęp do określonych danych, jeżeli jest w stanie udowodnić użytkownikowi lub osobie trzeciej, że mimo środków technicznych i organizacyjnych podjętych przez użytkownika lub osobę trzecią, istnieje duże prawdopodobieństwo, że ujawnienie tej tajemnicy przedsiębiorstwa poskutkuje poważną szkodą ekonomiczną. „Poważna szkoda ekonomiczna” oznacza poważne i nieodwracalne straty ekonomiczne. Posiadacz danych powinien bez zbędnej zwłoki należycie uzasadnić odmowę użytkownikowi lub osobie trzeciej na piśmie i powiadomić właściwy organ. Uzasadnienie powinno być oparte na obiektywnych elementach i wskazywać konkretne ryzyko poważnej szkody ekonomicznej, która ma wynikać z ujawnienia określonych danych, oraz powody, dla których środki podjęte dla ochrony żądanych danych nie są uznane za wystarczające. W tym kontekście można uwzględnić ewentualny negatywny wpływ na cyberbezpieczeństwo. Bez uszczerbku dla prawa dochodzenia roszczeń przed sądem lub trybunałem państwa członkowskiego, jeżeli użytkownik lub osoba trzecia chcą zaskarżyć decyzję posiadacza danych o odmowie, lub cofnąć lub zawiesić dzielenie się danymi, mogą oni złożyć skargę do właściwego organu, który bez zbędnej zwłoki powinien zdecydować, czy i na jakich warunkach należy rozpocząć lub wznowić dzielenie się danymi, lub uzgodnić z posiadaczem danych odesłanie sprawy do organu rozstrzygania sporów. Wyjątki od praw dostępu do danych przewidzianych w niniejszym rozporządzeniu w żadnym wypadku nie powinny ograniczać przysługujących osobom, których dane dotyczą, praw dostępu ani praw przenoszenia danych na podstawie rozporządzenia (UE) 2016/679.

(32) Celem niniejszego rozporządzenia jest nie tylko sprzyjanie opracowywaniu nowych, innowacyjnych produktów skomunikowanych lub usług powiązanych, pobudzanie innowacji na rynkach posprzedażowych, lecz także pobudzanie opracowywania zupełnie nowatorskich usług z wykorzystaniem określonych danych, w tym na podstawie danych z różnorodnych produktów skomunikowanych lub usług powiązanych. Jednocześnie celem niniejszego rozporządzenia jest uniknięcie osłabiania zachęt do inwestowania w ten rodzaj produktu skomunikowanego, z którego pozyskiwane są dane, np. w wyniku wykorzystywania danych do opracowania konkurencyjnego produktu skomunikowanego, który uznawany jest przez użytkowników za zamienny lub zastępowalny, w szczególności ze względu na jego cechy, cenę i zamierzony użytek. Niniejsze rozporządzenie nie zakazuje opracowywania usług powiązanych z wykorzystaniem danych pozyskanych na podstawie niniejszego rozporządzenia, ponieważ miałoby to niepożądany, zniechęcający wpływ na innowacje. Zakaz wykorzystywania danych, do których dostęp uzyskano na podstawie niniejszego rozporządzenia, do opracowania konkurencyjnego produktu skomunikowanego chroni wysiłki innowacyjne posiadacza danych. To, czy produkt skomunikowany konkuruje z produktem, z którego pochodzą dane, zależy od tego, czy oba produkty skomunikowane konkurują ze sobą na tym samym rynku produktowym. Należy to ustalić na podstawie ugruntowanych zasad unijnego prawa konkurencji służących definiowaniu stosownego rynku produktowego. Jednakże zgodnym z prawem celem wykorzystywania danych może być inżynieria odwrotna, o ile spełnia wymagania określone w niniejszym rozporządzeniu, prawie Unii lub prawie krajowym. Może tak być w przypadku celu, którym jest naprawa lub przedłużenie okresu trwałości produktu skomunikowanego, lub w przypadku świadczenia usług rynku posprzedażowego dla produktów skomunikowanych.

(33) Osobą trzecią, której udostępniane są dane, może być osoba fizyczna lub prawna, np. konsument, przedsiębiorstwo, organizacja badawcza, organizacja niekomercyjna lub podmiot działający w ramach swoich obowiązków zawodowych. Udostępniając dane osobie trzeciej, posiadacz danych nie powinien nadużywać swojej pozycji w celu uzyskania przewagi konkurencyjnej na rynkach, na których posiadacz danych i osoba trzecia mogą bezpośrednio ze sobą konkurować. Posiadacz danych nie powinien zatem wykorzystywać danych łatwo dostępnych do pozyskiwania informacji o sytuacji ekonomicznej takiej osoby trzeciej, jej aktywach lub metodach produkcji ani też nie powinien wykorzystywać takich danych w żaden inny sposób, który mógłby osłabić pozycję handlową osoby trzeciej na rynkach jej działalności. Użytkownik powinien móc dzielić się danymi nieosobowymi z osobami trzecimi w celach komercyjnych. Za zgodą użytkownika i z zastrzeżeniem przepisów niniejszego rozporządzenia osoby trzecie powinny móc przekazywać udostępnione przez użytkownika prawa dostępu do danych innym osobom trzecim, w tym za rekompensatą. Pośrednicy danych między przedsiębiorcami i systemy zarządzania informacjami osobowymi, określeni jako usługi pośrednictwa danych w rozporządzeniu (UE) 2022/868, mogą wspierać użytkowników lub osoby trzecie w ustanawianiu stosunków handlowych z nieokreśloną liczbą potencjalnych kontrahentów w jakimkolwiek zgodnym z prawem celu wchodzącym w zakres stosowania niniejszego rozporządzenia. Mogą oni odgrywać zasadniczą rolę w agregowaniu dostępu do danych, tak aby ułatwić analizę dużych zestawów danych lub uczenie się maszyn, pod warunkiem że użytkownicy zachowują pełną kontrolę nad wnoszeniem swoich danych do takiej agregacji, oraz nad warunkami handlowymi wykorzystywania ich danych.

(34) W wyniku korzystania z produktu skomunikowanego lub usługi powiązanej, zwłaszcza gdy użytkownikiem jest osoba fizyczna, mogą być generowane dane odnoszące się do osoby, której dane dotyczą. Przetwarzanie takich danych podlega zasadom określonym w rozporządzeniu (UE) 2016/679, w tym w przypadku gdy w zestawie danych dane osobowe i nieosobowe są ze sobą nierozerwalnie związane. Osobą, której dane dotyczą, może być użytkownik lub inna osoba fizyczna. Udostępnienia danych osobowych może żądać wyłącznie administrator danych lub osoba, której dane dotyczą. Użytkownik będący osobą, której dane dotyczą, w określonych okolicznościach ma na podstawie rozporządzenia (UE) 2016/679 prawo dostępu do dotyczących go danych osobowych, a niniejsze rozporządzenie nie ma wpływu na takie prawa. Zgodnie z niniejszym rozporządzeniem użytkownik będący osobą fizyczną ma również prawo dostępu do wszystkich danych, osobowych i nieosobowych, generowanych w czasie użytkowania produktu skomunikowanego. Użytkownik uznawany jest za administratora, w przypadku gdy użytkownikiem nie jest osoba, której dane dotyczą, tylko przedsiębiorstwo, w tym przedsiębiorca indywidualny, z wyłączeniem przypadków wspólnego użytkowania produktu skomunikowanego przez członków gospodarstwa domowego. W związku z tym, gdy taki użytkownik, jako administrator danych, zamierza zażądać danych osobowych generowanych w wyniku korzystania z produktu skomunikowanego lub usługi powiązanej, musi on mieć podstawę prawną do przetwarzania danych przewidzianą w art. 6 ust. 1 rozporządzenia (UE) 2016/679, taką jak zgoda osoby, której dane dotyczą, lub wykonanie umowy, którego stroną jest osoba, której dane dotyczą. Taki użytkownik powinien zapewnić, aby osoba, której dane dotyczą, została odpowiednio poinformowana o konkretnych, wyraźnych i prawnie uzasadnionych celach przetwarzania takich danych oraz o tym, w jaki sposób może skutecznie dochodzić swoich praw. Jeżeli posiadacz danych i użytkownik są współadministratorami w rozumieniu art. 26 rozporządzenia (UE) 2016/679, wówczas w drodze wspólnych uzgodnień w przejrzysty sposób muszą określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z tego rozporządzenia. Po udostępnieniu danych, uznaje się, że taki użytkownik może stać się posiadaczem danych, jeżeli spełnia kryteria określone w niniejszym rozporządzeniu, i tym samym będzie podlegać obowiązkom udostępniania danych określonym w niniejszym rozporządzeniu.

(35) Dane z produktu lub z usługi powiązanej należy udostępniać osobie trzeciej wyłącznie na wniosek użytkownika. Niniejsze rozporządzenie uzupełnia więc prawo przysługujące osobom, których dane dotyczą, przewidziane w art. 20 rozporządzenia (UE) 2016/679, do otrzymania danych ich dotyczących w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego i do przesłania tych danych innemu administratorowi, jeżeli dane te są przetwarzane w sposób zautomatyzowany na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) tego rozporządzenia. Osoby, których dane dotyczą, mają również prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.. W art. 20 rozporządzenia (UE) 2016/679 wskazano, że artykuł ten dotyczy danych dostarczonych przez osobę, której dane dotyczą, ale nie określono, czy wymaga to czynnego zachowania ze strony osoby, której dane dotyczą, czy też ma on zastosowanie również w sytuacjach, w których produkt skomunikowany lub usługa powiązana, ze względu na sposób swojego zaprojektowania, w bierny sposób rejestrują zachowanie osoby, której dane dotyczą, lub inne informacje związane z osobą, której dane dotyczą. Prawa przewidziane w niniejszym rozporządzeniu na różne sposoby uzupełniają prawo dostępu i przenoszenia danych osobowych na mocy art. 20 rozporządzenia (UE) 2016/679. Niniejsze rozporządzenie przyznaje użytkownikom prawo dostępu do danych z produktu lub z usługi powiązanej oraz prawo udostępniania takich danych osobie trzeciej, niezależnie od ich charakteru jako danych osobowych, podziału na dane czynnie dostarczane i dane rejestrowane w sposób bierny oraz niezależnie od podstawy prawnej przetwarzania. W przeciwieństwie do art. 20 rozporządzenia (UE) 2016/679 niniejsze rozporządzenie nakazuje i zapewnia techniczną możliwość dostępu osób trzecich do wszelkiego rodzaju danych objętych zakresem stosowania niniejszego rozporządzenia, niezależnie od tego, czy są to dane osobowe czy dane nieosobowe, a tym samym zapewnia, aby przeszkody techniczne nie utrudniały ani uniemożliwiały już dostępu do takich danych. Pozwala ono także posiadaczom danych określić zasadną rekompensatę uiszczaną przez osoby trzecie, ale nie przez użytkownika, z tytułu kosztów poniesionych w związku z udzieleniem bezpośredniego dostępu do danych generowanych przez produkt skomunikowany użytkownika. Brak porozumienia między posiadaczem danych a osobą trzecią co do warunków takiego bezpośredniego dostępu nie powinien w żaden sposób uniemożliwiać osobie, której dane dotyczą, wykonywania praw określonych w rozporządzeniu (UE) 2016/679, w tym prawa do przenoszenia danych, poprzez skorzystanie ze środków ochrony prawnej zgodnie z tym rozporządzeniem. W tym kontekście należy rozumieć, że zgodnie z rozporządzeniem (UE) 2016/679 umowa nie umożliwia posiadaczowi danych ani osobie trzeciej przetwarzania szczególnych kategorii danych osobowych.

(36) Dostęp do jakichkolwiek danych przechowywanych w urządzeniu końcowym i udostępnianych z tego urządzenia podlega przepisom dyrektywy 2002/58/WE i wymaga zgody abonenta lub użytkownika w rozumieniu tej dyrektywy, chyba że dostęp do takich danych jest ściśle niezbędny w celu świadczenia usługi społeczeństwa informacyjnego, której wyraźnie zażądali użytkownik lub abonent, lub jedynie w celu wykonania transmisji komunikatu. Dyrektywa 2002/58/WE chroni integralność końcowego urządzenia użytkownika w zakresie korzystania z możliwości przetwarzania i przechowywania oraz zbierania informacji. Urządzenie podłączone do internetu rzeczy uznaje się za urządzenie końcowe, jeżeli jest bezpośrednio lub pośrednio podłączone do publicznej sieci łączności.

(37) Aby nie dopuścić do nadużyć wobec użytkowników, osoby trzecie, którym udostępniono dane na wniosek użytkownika, powinny przetwarzać te dane wyłącznie do celów uzgodnionych z użytkownikiem i dzielić się nimi z inną osobą trzecią wyłącznie za zgodą użytkownika.

(38) Zgodnie z zasadą minimalizacji danych osoby trzecie powinny uzyskać dostęp wyłącznie do tych informacji, które są niezbędne do świadczenia usługi, której zażądał użytkownik. Po uzyskaniu dostępu do danych osoba trzecia powinna przetwarzać je do celów uzgodnionych z użytkownikiem bez ingerencji ze strony posiadacza danych. Odmówienie dostępu do danych osobie trzeciej przez użytkownika lub wycofanie przez użytkownika zgody na dostęp osoby trzeciej do danych powinno być tak samo proste, jak udzielenie zgody na taki dostęp przez użytkownika. Osoby trzecie i posiadacze danych nie powinni bezzasadnie utrudniać użytkownikom wykonywania praw lub dokonywania wyborów, w tym przez oferowanie użytkownikom wyboru w sposób nieneutralny, ani w żaden sposób zmuszać użytkownika, wprowadzać w błąd ani nim manipulować, ani podważać lub ograniczać autonomii, zdolności decyzyjnych lub wyborów użytkownika, w tym za pomocą interfejsu cyfrowego użytkownika lub jego części. W tym kontekście osoby trzecie lub posiadacze danych nie powinni podczas projektowania swoich interfejsów cyfrowych stosować tzw. zwodniczych interfejsów. Zwodnicze interfejsy to techniki projektowe służące do wymuszania na konsumentach decyzji, które mają dla nich negatywne skutki, lub wprowadzenia konsumentów w błąd w celu skłonienia ich do takich decyzji. Te techniki manipulacji mogą być wykorzystywane, by skłonić użytkowników, w szczególności konsumentów podatnych na zagrożenia, do niechcianych zachowań, wprowadzić ich błąd poprzez nakłanianie do decyzji w sprawie udostępnienia danych lub też by nieobiektywnie wpłynąć na zdolności decyzyjne użytkowników usługi w sposób podważający lub ograniczający ich autonomię, zdolności decyzyjne i wybór. Powszechne i uzasadnione praktyki handlowe zgodne z prawem Unii nie powinny same w sobie być uznawane za zwodnicze interfejsy. Osoby trzecie i posiadacze danych powinni wywiązywać się ze swoich obowiązków określonych w stosownym prawie Unii, w szczególności z wymagań określonych w dyrektywach Parlamentu Europejskiego i Rady 98/6/WE[1] i 2000/31/WE[2], oraz dyrektywach 2005/29/WE i 2011/83/UE.

---

[1] Dyrektywa 98/6/WE Parlamentu Europejskiego i Rady z dnia 16 lutego 1998 r. w sprawie ochrony konsumenta przez podawanie cen produktów oferowanych konsumentom (Dz.U. L 80 z 18.3.1998, s. 27).

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

(39) Osoby trzecie nie powinny ponadto wykorzystywać danych wchodzących w zakres stosowania niniejszego rozporządzenia do profilowania osób fizycznych, chyba że takie czynności przetwarzania są ściśle niezbędne do świadczenia usługi, której zażądał użytkownik, w tym w ramach zautomatyzowanego podejmowania decyzji. Wymaganie usunięcia danych, które nie są już niezbędne do celu uzgodnionego z użytkownikiem, o ile w odniesieniu do danych nieosobowych uzgodniono inaczej, stanowi uzupełnienie prawa do usunięcia danych przysługującego osobie, której dane dotyczą, na podstawie art. 17 rozporządzenia (UE) 2016/679. W przypadku gdy osoba trzecia jest dostawcą usługi pośrednictwa, zastosowanie mają zabezpieczenia wobec osoby, której dane dotyczą, przewidziane w rozporządzeniu (UE) 2022/868. Osoba trzecia może wykorzystywać dane do opracowania nowego, innowacyjnego produktu skomunikowanego lub nowej, innowacyjnej usługi powiązanej, lecz nie do opracowania konkurencyjnego produktu skomunikowanego.

(40) Przedsiębiorstwom typu start-up, małym przedsiębiorstwom, przedsiębiorstwom, które kwalifikują się jako średnie przedsiębiorstwa zgodnie z art. 2 załącznika do zalecenia 2003/361/WE, oraz przedsiębiorstwom z tradycyjnych sektorów o mniej rozwiniętych zdolnościach cyfrowych trudno jest uzyskać dostęp do istotnych danych. Niniejsze rozporządzenie ma na celu ułatwienie dostępu do danych takim podmiotom, a jednocześnie zapewnienie, aby odpowiednie obowiązki były jak najbardziej proporcjonalne w celu uniknięcia nadmiernego obciążenia regulacyjnego. Ponadto pojawiła się niewielka liczba bardzo dużych przedsiębiorstw posiadających znaczną siłę gospodarczą w gospodarce cyfrowej dzięki koncentracji i agregacji wielkich ilości danych oraz dzięki infrastrukturze technicznej pozwalającej na czerpanie z nich korzyści finansowych. Te bardzo duże przedsiębiorstwa obejmują przedsiębiorstwa świadczące podstawowe usługi platformowe kontrolujące całe ekosystemy platformowe w gospodarce cyfrowej, z którymi to przedsiębiorstwami istniejący lub nowi uczestnicy rynku nie są w stanie konkurować ani którym nie są w stanie zagrozić. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925[1] ma skorygować te braki i zakłócenia równowagi poprzez umożliwienie Komisji wskazania przedsiębiorstwa jako „strażnika dostępu”; określa ono szereg obowiązków takich strażników dostępu, w tym zakaz łączenia niektórych danych bez uzyskania zgody oraz obowiązek zapewnienia skutecznych praw do przenoszenia danych zgodnie z art. 20 rozporządzenia (UE) 2016/679. Zgodnie z rozporządzeniem (UE) 2022/1925 i mając na uwadze bezkonkurencyjną zdolność tych przedsiębiorstw do pozyskiwania danych, uwzględnienie strażników dostępu wśród beneficjentów prawa dostępu do danych nie jest niezbędne do osiągnięcia celu niniejszego rozporządzenia i tym samym byłoby nieproporcjonalne dla posiadaczy danych, na których ciążą takie obowiązki.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.U. L 265 z 12.10.2022, s. 1).

Takie uwzględnienie strażników dostępu mogłoby także ograniczyć korzyści wynikające z niniejszego rozporządzenia dla MŚP w zakresie sprawiedliwej dystrybucji wartości danych wśród uczestników rynku. Oznacza to, że przedsiębiorstwo świadczące podstawowe usługi platformowe, które zostało wskazane jako strażnik dostępu, nie może żądać ani uzyskiwać dostępu do danych użytkownika generowanych w wyniku korzystania z produktu skomunikowanego, usługi powiązanej lub wirtualnego asystenta zgodnie z niniejszym rozporządzeniem. Ponadto osoby trzecie, którym udostępniane są dane na wniosek użytkownika, nie mogą udostępniać tych danych strażnikowi dostępu. Na przykład osoba trzecia nie może zlecić strażnikowi dostępu podwykonawstwa świadczenia usługi. Nie oznacza to jednak, że osoby trzecie nie mogą korzystać z usług przetwarzania danych oferowanych przez strażnika dostępu. Nie uniemożliwia to także tym przedsiębiorstwom pozyskiwania ani wykorzystywania tych samych danych innymi zgodnymi z prawem sposobami. Prawa dostępu określone w niniejszym rozporządzeniu pomagają w zapewnieniu konsumentom szerszego wyboru usług. Ponieważ możliwość zawarcia dobrowolnej umowy między strażnikami dostępu a posiadaczami danych pozostaje nienaruszona, ograniczenie udzielania dostępu strażnikom dostępu nie wykluczałoby ich z rynku ani nie uniemożliwiałoby im oferowania usług**.**

(41) Biorąc pod uwagę obecny stan rozwoju technologii, nakładanie dalszych obowiązków w zakresie projektowania produktów skomunikowanych produkowanych lub projektowanych przez mikroprzedsiębiorstwa i małe przedsiębiorstwa lub usług powiązanych świadczonych przez takie przedsiębiorstwa wiązałoby się dla nich z nadmiernym obciążeniem. Nie dotyczy to jednak sytuacji, w której mikroprzedsiębiorstwo lub małe przedsiębiorstwo ma przedsiębiorstwo partnerskie lub przedsiębiorstwo powiązane w rozumieniu w art. 3 załącznika do zalecenia Komisji 2003/361/WE, które nie kwalifikuje się jako mikroprzedsiębiorstwo lub małe przedsiębiorstwo, i któremu zostaje zlecone wyprodukowanie lub zaprojektowanie produktu skomunikowanego lub świadczenie usługi powiązanej w ramach podwykonawstwa. W takich sytuacjach przedsiębiorstwo, które zleciło produkcję lub projekt w ramach podwykonawstwa mikroprzedsiębiorstwu lub małemu przedsiębiorstwu, jest w stanie zapewnić podwykonawcy odpowiednią rekompensatę. Mikroprzedsiębiorstwo lub małe przedsiębiorstwo, jeżeli nie jest producentem produktu skomunikowanego ani dostawcą usług powiązanych, może jednak podlegać wymaganiom ustanowionym w niniejszym rozporządzeniu jako posiadacz danych. Okres przejściowy powinien mieć zastosowanie do przedsiębiorstwa, które kwalifikuje się jako średnie przedsiębiorstwo przez okres krótszy niż rok, a także do produktów skomunikowanych przez okres jednego roku od dnia wprowadzenia ich do obrotu przez średnie przedsiębiorstwo. Taki roczny okres przejściowy umożliwia średniemu przedsiębiorstwu dostosowanie się i przygotowanie przed zmierzeniem się z konkurencją na rynku usług dla produktów skomunikowanych, które produkuje, na podstawie praw dostępu określonych w niniejszym rozporządzeniu. Ten okres przejściowy nie ma zastosowania w przypadku gdy takie średnie przedsiębiorstwo ma przedsiębiorstwo partnerskie lub przedsiębiorstwo powiązane, które nie kwalifikuje się jako mikroprzedsiębiorstwo lub małe przedsiębiorstwo, i gdy takiemu średniemu przedsiębiorstwu zostało zlecone wyprodukowanie lub zaprojektowanie produktu skomunikowanego lub świadczenie usługi powiązanej w ramach podwykonawstwa.

(42) Aby uwzględnić liczne produkty skomunikowane generujące dane o różnym charakterze, ilości i częstotliwości, stwarzające różny poziom ryzyka związanego z danymi i z cyberbezpieczeństwem oraz oferujące możliwości ekonomiczne o różnej wartości oraz aby zapewnić spójność praktyk w ramach dzielenia się danymi na rynku wewnętrznym, w tym między sektorami, i zachęcać do stosowania uczciwych praktyk dzielenia się danymi i promować takie praktyki nawet w dziedzinach, w których takie prawo dostępu do danych nie jest przewidziane, niniejsze rozporządzenie przewiduje horyzontalne zasady w sprawie uzgodnień dotyczących dostępu do danych, gdy posiadacz danych jest zobowiązany z mocy prawa Unii lub prawa krajowego przyjętego zgodnie z prawem Unii do udostępnienia danych odbiorcy danych. Takiego dostępu należy udzielać na sprawiedliwych, uzasadnionych, niedyskryminacyjnych i przejrzystych zasadach. Takie ogólne zasady dostępu nie mają zastosowania do obowiązków udostępniania danych na podstawie rozporządzenia (UE) 2016/679. Zasady te nie mają wpływu na dobrowolne dzielenie się danymi. Niewiążące modelowe postanowienia umowne dotyczące dzielenia się danymi między przedsiębiorcami, które zostaną opracowane i będą zalecane przez Komisję mogą pomóc stronom w zawieraniu umów, które będą przewidywać sprawiedliwe, uzasadnione i niedyskryminacyjne zasady i będą wdrażane w sposób przejrzysty. Zawarcie umów, które mogą zawierać nieważące modelowe postanowienia umowne, nie powinno oznaczać, że prawo do dzielenia się danymi z osobami trzecimi w jakikolwiek sposób zależy od istnienia takiej umowy. Gdyby strony nie były w stanie zawrzeć umowy o dzieleniu się danymi, w tym przy wsparciu organów rozstrzygania sporów, prawa do dzielenia się danymi z osobami trzecimi można dochodzić w sądach i trybunałach krajowych.

(43) Na podstawie zasady swobody zawierania umów strony powinny nadal móc swobodnie ustalać szczegółowe warunki udostępniania danych w ich umowach, w ramach ogólnych zasad dostępu dotyczących udostępniania danych. Wśród warunków takich umów mogą się znaleźć środki techniczne i organizacyjne, w tym te związane z bezpieczeństwem danych.

(44) W celu zapewnienia, aby warunki obowiązkowego dostępu do danych były sprawiedliwe dla obu stron umowy, ogólne zasady dotyczące praw dostępu do danych powinny odnosić się do zasady unikania nieuczciwych postanowień umownych.

(45) Umowa zawarta w stosunkach między przedsiębiorcami w celu udostępniania danych nie powinna rozróżniać porównywalnych kategorii odbiorców danych, niezależnie od tego, czy stronami są duże przedsiębiorstwa czy MŚP. Ponieważ brak informacji na temat warunków poszczególnych umów utrudnia odbiorcom ocenę, czy warunki udostępniania danych są niedyskryminacyjne, ciężar dowodu, że postanowienia umowne są niedyskryminacyjne powinien spoczywać na posiadaczach danych. Stosowanie przez posiadacza danych różnych postanowień umownych dotyczących udostępniania danych nie stanowi niezgodnej z prawem dyskryminacji, jeżeli różnice te są uzasadnione obiektywnymi względami. Obowiązki te pozostają bez uszczerbku dla rozporządzenia (UE) 2016/679.

(46) Aby zachęcać do dalszych inwestycji w generowanie i udostępnianie wartościowych danych, w tym do inwestycji w stosowne narzędzia techniczne, a jednocześnie zapobiegać nadmiernym obciążeniom w zakresie dostępu do danych i ich wykorzystywania, w wyniku których dzielenie się danymi nie jest opłacalne, niniejsze rozporządzenie zawiera zasadę, zgodnie z którą w stosunkach między przedsiębiorcami posiadacze danych mogą zażądać zasadnej rekompensaty, gdy są zobowiązani zgodnie z prawem Unii lub prawem krajowym przyjętym zgodnie z prawem Unii do udostępnienia danych odbiorcy danych. |Rekompensaty takiej nie należy rozumieć jako płatności za same dane. Komisja powinna przyjąć wytyczne w sprawie obliczania zasadnej rekompensaty w gospodarce opartej na danych.

(47) Po pierwsze, zasadna rekompensata za wywiązanie się z obowiązku zastosowania się do wniosku o udostępnienie danych, zgodnie z prawem Unii lub prawem krajowym przyjętym zgodnie z prawem Unii, może obejmować rekompensatę za poniesione koszty udostępnienia danych. Do kosztów tych mogą należeć koszty techniczne, np. takie, które trzeba ponieść w związku ze zwielokrotnieniem danych, rozpowszechnieniem danych za pomocą środków elektronicznych i przechowywaniem danych, ale nie ze zbieraniem lub tworzeniem danych. Takie koszty techniczne mogą obejmować również koszty przetwarzania niezbędne do udostępnienia danych, w tym koszty związane z formatowaniem danych. Koszty związane z udostępnieniem danych mogą również obejmować koszty odpowiadania na konkretne wnioski o udostępnienie danych. Mogą też być zróżnicowane zależnie od ilości danych oraz od przyjętych uzgodnień dotyczących udostępnienia danych. Długoterminowe uzgodnienia między posiadaczami danych a odbiorcami danych, np. w formie modelu abonenckiego lub inteligentnych umów, mogłyby obniżyć koszty regularnych lub powtarzających się transakcji w stosunkach między przedsiębiorcami. Koszty związane z udostępnieniem danych są albo szczególne dla danego wniosku, albo dzielone z innymi wnioskami. W tym drugim przypadku pojedynczy odbiorca danych nie powinien ponosić pełnych kosztów udostępnienia danych. Po drugie, zasadna rekompensata może obejmować też marżę, z wyjątkiem w odniesieniu do MŚP i niekomercyjnych organizacji badawczych. Marża może być zróżnicowana zależnie od czynników związanych z samymi danymi, takich jak ilość, format lub charakter danych. Może uwzględniać także koszty zebrania danych. Marża może zatem być mniejsza, gdy posiadacz danych zebrał dane na potrzeby własnej działalności bez znacznych inwestycji, lub może być większa, gdy inwestycje w zebranie danych do celów działalności posiadacza danych są znaczne. Może być ona ograniczona lub nawet wyłączona w sytuacjach, w których wykorzystanie danych przez odbiorcę danych nie wpływa na działalność posiadacza danych. Fakt, że dane są współgenerowane przez produkt skomunikowany należący do użytkownika, wzięty przez niego w najem, w dzierżawę lub w leasing, może również obniżyć wysokość rekompensaty w porównaniu z innymi sytuacjami, w których dane są generowane wyłącznie przez posiadacza danych, np. w trakcie świadczenia usługi powiązanej.

(48) Nie ma potrzeby interwencji w przypadku dzielenia się danymi między dużymi przedsiębiorstwami lub w przypadku, w którym posiadaczem danych jest małe lub średnie przedsiębiorstwo, a odbiorcą danych – duże przedsiębiorstwo. W takich przypadkach uznaje się, że przedsiębiorstwa są w stanie wynegocjować zasadną i niedyskryminującą rekompensatę.

(49) Na potrzeby ochrony MŚP przed nadmiernymi obciążeniami ekonomicznymi, przez które przedsiębiorstwom tym z handlowego punktu widzenia byłoby zbyt trudno opracowywać i realizować innowacyjne modele biznesowe, wypłacana przez nie zasadna rekompensata za udostępnienie danych nie powinno przekraczać kosztu bezpośrednio związanego z udostępnieniem tych danych. Ten sam system powinien mieć zastosowanie do niekomercyjnych organizacji badawczych.

(50) W należycie uzasadnionych przypadkach, w tym w przypadku gdy istnieje potrzeba zapewnienia udziału konsumentów i konkurencyjności lub promowania innowacyjności na niektórych rynkach, można uregulować rekompensatę za udostępnianie określonych rodzajów danych w prawie Unii lub prawie krajowym przyjętym zgodnie z prawem Unii.

(51) Przejrzystość stanowi ważną zasadę potrzebną do zapewnienia, aby rekompensata żądana przez posiadacza danych była zasadna lub – jeżeli odbiorcą danych jest MŚP lub niekomercyjna organizacja badawcza – aby rekompensata nie przekraczała kosztów bezpośrednio związanych z udostępnieniem danych odbiorcy danych i wiązała się z konkretnym wnioskiem. Aby odbiorcy danych byli w stanie ocenić i zweryfikować, czy rekompensata spełnia wymagania określone w niniejszym rozporządzeniu, posiadacz danych powinien przedstawić odbiorcy danych informacje na tyle szczegółowe, aby można było obliczyć tę rekompensatę.

(52) Zapewnienie dostępu do alternatywnych metod rozwiązywania krajowych i transgranicznych sporów związanych z udostępnianiem danych powinno być korzystne dla posiadaczy danych i odbiorców danych, i tym samym powinno skutkować wzrostem wiarygodności dzielenia się danymi. Jeżeli strony nie są w stanie uzgodnić sprawiedliwych, rozsądnych i niedyskryminujących zasad udostępniania danych, organy rozstrzygania sporów powinny zaoferować stronom proste, szybkie i tanie rozwiązanie. Niniejsze rozporządzenie ustanawia jedynie warunki, które muszą zostać spełnione przez organy rozstrzygania sporów, aby uzyskać certyfikację, państwa członkowskie mogą jednak przyjąć szczególne zasady procedury certyfikacji, w tym wygaśnięcia lub cofnięcia certyfikacji. Przepisy niniejszego rozporządzenia dotyczące rozstrzygania sporów nie powinny nakładać na państwa członkowskie obowiązku ustanowienia organów rozstrzygania sporów.

(53) Procedura rozstrzygania sporów przewidziana w niniejszym rozporządzeniu jest procedurą dobrowolną, umożliwiającą użytkownikom, posiadaczom danych i odbiorcom danych ustalenie, że ich spór zostanie wniesiony do organu rozstrzygania sporów. Dlatego strony powinny móc zwrócić się do wybranego przez siebie organu rozstrzygania sporów w państwach członkowskich, w których strony mają siedzibę, lub poza tymi państwami.

(54) Aby zapobiec przypadkom, w których ten sam spór zostaje skierowany do dwóch lub więcej organów rozstrzygania sporów, w szczególności w sytuacji transgranicznej, organ rozstrzygania sporów powinien móc odrzucić wniosek o rozwiązanie sporu, który został już przedstawiony innemu organowi rozstrzygania sporów bądź sądowi lub trybunałowi państwa członkowskiego.

(55) Aby zapewnić jednolite stosowanie niniejszego rozporządzenia, organy rozstrzygania sporów powinny uwzględniać niewiążące modelowe postanowienia umowne, które zostaną opracowane i będą zalecane przez Komisję, oraz prawo Unii lub prawo krajowe doprecyzowujące obowiązki dzielenia się danymi lub wytyczne organów sektorowych w sprawie stosowania takiego prawa.

(56) Stronom postępowania w sprawie rozstrzygnięcia sporu nie należy uniemożliwiać wykonania przysługującego im podstawowego prawa do skutecznego środka prawnego i sprawiedliwego procesu. Dlatego też decyzja o przekazaniu sporu do organu rozstrzygającego spory nie powinna skutkować utratą przez takie strony prawa do dochodzenia roszczeń przed sądem lub trybunałem państwa członkowskiego. Organy rozstrzygania sporów powinny podawać do wiadomości publicznej roczne sprawozdania z działalności.

(57) Posiadacze danych mogą stosować odpowiednie techniczne środki ochrony, aby zapobiegać niezgodnemu z prawem ujawnianiu danych i dostępowi do danych. Środki te nie powinny jednak powodować nierównego traktowania odbiorców danych ani utrudniać użytkownikom lub odbiorcom danych dostępu do danych lub ich wykorzystywania. W przypadku nadużyć ze strony odbiorcy danych, np. wprowadzenia posiadacza danych w błąd poprzez przedstawienie fałszywych informacji w celu wykorzystania danych do celów niezgodnych z prawem, w tym opracowania na podstawie tych danych konkurencyjnego produktu skomunikowanego, posiadacz danych oraz, w stosownych przypadkach i w przypadku gdy nie są one tą samą osobą, posiadacz tajemnicy przedsiębiorstwa lub użytkownik mogą wystąpić do osoby trzeciej lub odbiorcy danych z wnioskiem o zastosowanie bez zbędnej zwłoki środków naprawczych lub zaradczych. Wszelkie takie wnioski, w szczególności wnioski o zaprzestanie produkcji, oferowania lub wprowadzania do obrotu towarów, danych wywnioskowanych lub usług oraz o zaprzestanie przywozu, wywozu, magazynowania towarów naruszających prawo lub o ich zniszczenie, powinny być oceniane w świetle ich proporcjonalności w stosunku do interesów posiadacza danych, posiadacza tajemnic przedsiębiorstwa lub użytkownika.

(58) W przypadku gdy jedna ze stron ma silniejszą pozycję negocjacyjną, istnieje ryzyko, że strona ta wykorzysta swoją pozycję ze szkodą dla drugiej umawiającej się strony w ramach negocjowania dostępu do danych i sprawi, że dostęp do danych będzie komercyjnie mniej opłacalny, a czasem nawet ekonomicznie zaporowy. Taki brak równowagi kontraktowej jest szkodliwy dla wszystkich przedsiębiorstw nieposiadających rzeczywistej możliwości negocjowania warunków dostępu do danych, które to przedsiębiorstwa ze względu na brak wyboru mogą być zmuszone do zaakceptowania postanowień umownych oferowanych na zasadzie „przyjmij albo zrezygnuj”. Z tego względu nieuczciwe postanowienia umowne regulujące dostęp do danych i ich wykorzystywanie lub regulujące odpowiedzialność i środki ochrony prawnej wobec naruszenia lub odstąpienia od obowiązków dotyczących danych nie powinny być dla przedsiębiorstw wiążące, jeżeli postanowienia te zostały na nie nałożone jednostronnie.

(59) W przepisach dotyczących postanowień umownych należy uwzględnić zasadę swobody zawierania umów, będącą podstawową ideą stosunków między przedsiębiorcami. Dlatego też analizie nieuczciwego charakteru powinny podlegać nie wszystkie postanowienia umowne, ale wyłącznie te, które zostały nałożone jednostronnie. Dotyczy to zasady „przyjmij albo zrezygnuj”, w której to sytuacji dany przedsiębiorca nie jest w stanie wywrzeć wpływu na treść postanowienia umownego zaproponowanego przez drugą stronę pomimo prób negocjacji w jego sprawie. Za postanowienie umowne nałożone jednostronnie nie należy uznawać postanowienia, które zostało po prostu przedstawione przez jedną stronę i zaakceptowane przez drugiego przedsiębiorcę ani też postanowienia wynegocjowanego i następnie przyjętego po zmianach przez umawiające się strony.

(60) Ponadto zasady dotyczące nieuczciwych postanowień umownych powinny mieć zastosowanie wyłącznie do elementów umowy związanych z udostępnianiem danych, tj. do postanowień umownych dotyczących dostępu do danych i ich wykorzystywania oraz odpowiedzialności lub środków ochrony prawnej wobec naruszenia i odstąpienia od obowiązków dotyczących danych. Analiza nieuczciwego charakteru ustanowiona w niniejszym rozporządzeniu nie powinna mieć zastosowania do innych części tej samej umowy, niezwiązanych z udostępnianiem danych.

(61) Kryteria służące do identyfikacji nieuczciwych postanowień umownych należy stosować wyłącznie wobec nieproporcjonalnych postanowień umownych, w przypadku których doszło do nadużycia silniejszej pozycji negocjacyjnej. Zdecydowana większość postanowień umownych, które w kontekście handlowym są korzystniejsze dla jednej ze stron, w tym postanowienia zwykle występujące w umowach między przedsiębiorcami, zwyczajnie odzwierciedla zasadę swobody zawierania umów i nadal obowiązuje. Do celów niniejszego rozporządzenia rażące odstępstwo od dobrej praktyki handlowej obejmuje m.in. obiektywne zmniejszenie zdolności strony, na którą jednostronnie nałożone zostało postanowienie, do ochrony uzasadnionego interesu handlowego leżącego w przedmiotowych danych.

(62) Aby zagwarantować pewność prawa, ustanawia się w niniejszym rozporządzeniu wykaz postanowień umownych, które bez wyjątku uznaje się za nieuczciwe, oraz wykaz postanowień umownych, w odniesieniu do których domniemywa się, że są nieuczciwe. W tym drugim przypadku przedsiębiorstwo, które nakłada dane postanowienie umowne, powinno być w stanie obalić domniemanie nieuczciwości, wykazując, że w konkretnym przypadku postanowienie wymienione w niniejszym rozporządzeniu nie jest nieuczciwe. Jeżeli postanowienie umowne nie widnieje w wykazie postanowień, które zawsze uznaje się za nieuczciwe albo w odniesieniu do których domniemywa się, że są nieuczciwe, zastosowanie ma ogólny przepis dotyczący nieuczciwego charakteru. W tym względzie postanowienia umowne wymienione w niniejszym rozporządzeniu jako postanowienia nieuczciwe powinny służyć jako kryteria interpretacji ogólnego przepisu dotyczącego nieuczciwego charakteru. Ponadto w negocjowaniu umów mogą pomóc stronom będącym podmiotami prowadzącymi działalność gospodarczą także opracowane i zalecane przez Komisję niewiążące modelowe postanowienia umowne dla umów między przedsiębiorcami w sprawie dzielenia się danymi. Jeżeli postanowienie umowne zostaje uznane za nieuczciwe, dana umowa powinna nadal obowiązywać bez tego postanowienia, chyba że nie można go oddzielić od pozostałych postanowień umownych.

(63) W sytuacji wyjątkowej potrzeby niezbędne może być wykorzystanie przez organy sektora publicznego, Komisję, Europejski Bank Centralny lub organy Unii istniejących danych, w tym w stosownym przypadku powiązanych metadanych, w celu wykonania ustawowych obowiązków realizowanych w interesie publicznym, aby zareagować na niebezpieczeństwo publiczne lub w innych wyjątkowych przypadkach. Wyjątkowe potrzeby to okoliczności nieprzewidziane i ograniczone w czasie w przeciwieństwie do innych okoliczności, które mogą być zaplanowane, wyznaczone, okresowe lub częste. Pojęcie „posiadacz danych" zasadniczo nie obejmuje organów sektora publicznego, może ono jednak obejmować przedsiębiorstwa publiczne. Organizacje prowadzące badania naukowe i organizacje finansujące badania naukowe także mogą być organami sektora publicznego lub podmiotami prawa publicznego. Aby ograniczyć ciężar spoczywający na przedsiębiorstwach, mikroprzedsiębiorstwa i małe przedsiębiorstwa powinny podlegać obowiązkowi dostarczenia danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organom Unii wyłącznie w sytuacjach wyjątkowej potrzeby, w przypadku gdy takie dane są niezbędne w celu zareagowania na niebezpieczeństwo publiczne a organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii nie są w stanie uzyskać takich danych za pomocą alternatywnych środków w sposób terminowy i skuteczny na równoważnych warunkach.

(64) W przypadku niebezpieczeństwa publicznego, takiego jak stan zagrożenia zdrowia publicznego, sytuacje wyjątkowe związane z klęskami żywiołowymi, w tym sytuacje pogarszane przez zmianę klimatu i degradację środowiska, oraz poważne katastrofy spowodowane przez człowieka, takie jak poważne cyberincydenty, interes publiczny wynikający z wykorzystania danych będzie nadrzędny względem interesów posiadacza danych związanych ze swobodnym dysponowaniem danymi, które są w jego posiadaniu. W takim przypadku posiadacze danych powinni być zobowiązani do udostępnienia danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organom Unii na ich wniosek. Występowanie niebezpieczeństwa publicznego należy ustalić lub ogłosić zgodnie z prawem Unii lub prawem krajowym na podstawie odpowiednich procedur, w tym procedur stosowanych przez odpowiednie organizacje międzynarodowe. W takich przypadkach organ sektora publicznego powinien wykazać, że w przeciwnym razie danych objętych wnioskiem nie da się pozyskać na czas, skutecznie i na równoważnych warunkach, np. w wyniku ich dobrowolnego dostarczenia przez inne przedsiębiorstwo lub w wyniku kwerendy w publicznej bazie danych.

(65) Wyjątkowa potrzeba może wynikać również z sytuacji innych niż niebezpieczne. W takich przypadkach organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii powinny mieć możliwość występowania z wnioskiem wyłącznie o dane nieosobowe. Organ sektora publicznego powinien wykazać, że dane są niezbędne do realizacji konkretnego zadania realizowanego w interesie publicznym, które zostało wyraźnie przewidziane prawem, takiego jak tworzenie statystyki publicznej lub łagodzenie stanu niebezpieczeństwa publicznego lub przywrócenie stanu wyjściowego po jego wystąpieniu. Ponadto z takim wnioskiem można wystąpić wyłącznie wtedy, gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii zidentyfikują konkretne dane, których w przeciwnym razie nie da się pozyskać na czas, skutecznie i na równoważnych warunkach, i wyłącznie wtedy, gdy wyczerpią wszystkie inne dostępne im sposoby pozyskiwania takich danych, takie jak pozyskanie danych na podstawie dobrowolnych umów, w tym zakup danych nieosobowych na rynku poprzez zaoferowanie stawek rynkowych, lub odwołanie się do istniejących obowiązków udostępnienia danych, lub przyjęcie nowych środków ustawodawczych, które mogłyby zagwarantować dostępność danych na czas. Zastosowanie powinny mieć zasady dotyczące wniosków, takie jak te związane z ograniczeniem celu, proporcjonalnością, przejrzystością oraz ograniczeniem w czasie. W przypadku wniosków o dane niezbędne do tworzenia statystyki publicznej organ sektora publicznego występujący z wnioskiem powinien także wykazać, czy prawo krajowe pozwala mu zakupić dane nieosobowe na rynku.

(66) Niniejsze rozporządzenie nie powinno dotyczyć ani wykluczać dobrowolnych uzgodnień dotyczących wymiany danych między podmiotami prywatnymi i publicznymi, w tym dotyczących dostarczania danych przez MŚP, i pozostaje bez uszczerbku dla aktów prawnych Unii ustanawiających obowiązkowe wnioski o udzielenie informacji kierowane przez podmioty publiczne do podmiotów prywatnych. Niniejsze rozporządzenie nie powinno wpływać na obowiązki posiadaczy danych dotyczące dostarczania danych w sytuacjach, w których nie zachodzi wyjątkowa potrzeba, w szczególności gdy zakres danych i posiadaczy danych jest znany lub gdy wykorzystywanie danych może odbywać się regularnie, tak jak ma to miejsce w przypadku obowiązków sprawozdawczych i obowiązków związanych z rynkiem wewnętrznym. Niniejsze rozporządzenie nie powinno również wpływać na wymagania dotyczące dostępu do danych w celu weryfikacji przestrzegania mających zastosowanie przepisów, w tym w przypadkach, w których organy sektora publicznego zlecają przeprowadzenie weryfikacji jednostkom niebędącym organami sektora publicznego.

(67) Niniejsze rozporządzenie uzupełnia prawo Unii i prawo krajowe przewidujące dostęp do danych i ich wykorzystywanie w celach statystycznych i pozostaje bez uszczerbku dla tego prawa, w szczególności rozporządzenia Parlamentu Europejskiego (WE) 223/2009[1] oraz krajowych aktów prawnych dotyczących statystyki publicznej.

(68) Do celów realizacji zadań w obszarze zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych, wykonywania sankcji karnych i administracyjnych, a także zbierania danych do celów celnych lub podatkowych organy sektora publicznego, Komisja, Europejski Bank Centralny lub organy Unii powinny korzystać z uprawnień nadanych im na mocy prawa Unii lub prawa krajowego.. Niniejsze rozporządzenie nie wpływa zatem na akty prawne dotyczące dzielenia się danymi, uzyskiwania do nich dostępu i ich wykorzystywania w tych obszarach.

---

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

(69) Zgodnie z art. 6 ust. 1 i 3 rozporządzenia (UE) 2016/679 do określenia podstawy prawnej udostępnienia danych przez posiadaczy danych – w przypadku wyjątkowej potrzeby – organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organom Unii niezbędne są na poziomie Unii proporcjonalne, ograniczone i przewidywalne ramy zarówno w celu zagwarantowania pewności prawa, jak i ograniczenia do minimum obciążeń administracyjnych nakładanych na przedsiębiorców. W tym celu wnioski o dane od organów sektora publicznego, Komisji, Europejskiego Banku Centralnego lub organów Unii do posiadaczy danych powinny być konkretne, przejrzyste i proporcjonalne pod względem zakresu treści i poziomu szczegółowości. Należy wyraźnie i konkretnie wskazać cel wniosku i planowane wykorzystanie żądanych danych, a jednocześnie dopuścić odpowiednią elastyczność, tak aby podmiot występujący z wnioskiem mógł zrealizować swoje określone zadania realizowane w interesie publicznym. We wniosku należy również wziąć pod uwagę uzasadnione interesy posiadacza danych będącego adresatem wniosku. Należy ograniczyć do minimum ciężar nakładany na posiadaczy danych poprzez zobowiązanie podmiotów występujących z wnioskiem do przestrzegania zasady jednorazowości, która zapobiega wielokrotnemu występowaniu o te same dane przez więcej niż jeden organ sektora publicznego, lub Komisję, Europejski Bank Centralny lub organ Unii. Aby zapewnić przejrzystość, wnioski o dane od Komisji, Europejskiego Banku Centralnego lub organów Unii powinny zostać bez zbędnej zwłoki podane do wiadomości publicznej przez podmiot występujący z wnioskiem o dane. Europejski Bank Centralny lub organy Unii powinny informować Komisję o ich wnioskach o dane. W przypadku gdy z wnioskiem o dane wystąpił organ sektora publicznego, organ ten powinien także powiadomić koordynatora danych państwa członkowskiego, w którym ma siedzibę organ sektora publicznego. Należy zapewnić, aby wszystkie wnioski były publicznie dostępne w internecie. Po otrzymaniu powiadomienia dotyczącego wniosku o dane właściwy organ może zdecydować o poddaniu wniosku ocenie, czy jest on zgodny z prawem, i wykonać swoje funkcje związane z egzekwowaniem i stosowaniem niniejszego rozporządzenia. Koordynator danych powinien zapewnić, by wszystkie wnioski, z którymi wystąpiły organy sektora publicznego, były publicznie dostępne w internecie.

(70) Celem obowiązku dostarczania danych jest zapewnienie, aby organy sektora publicznego, Komisja, Europejski Bank Centralny lub organy Unii dysponowały niezbędną wiedzą pozwalającą reagować na niebezpieczeństwa publiczne, zapobiegać im lub przywracać stan wyjściowy po wystąpieniu niebezpieczeństwa publicznego lub utrzymywać zdolność do realizacji konkretnych zadań wyraźnie określonych w prawie. Wśród danych pozyskiwanych przez te podmioty mogą znajdować się szczególnie chronione informacje handlowe. Z tego względu do danych udostępnianych na podstawie niniejszego rozporządzenia nie powinny mieć zastosowania ani rozporządzenie (UE) 2022/868, ani dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024[1], i nie należy uznawać, że są to otwarte dane, które mogą być ponownie wykorzystywane przez osoby trzecie. Nie powinno to jednak wpływać na stosowanie dyrektywy (UE) 2019/1024 do ponownego wykorzystywania statystyki publicznej, przy której tworzeniu wykorzystano dane pozyskane na podstawie niniejszego rozporządzenia, pod warunkiem że ponowne wykorzystanie nie dotyczy danych bazowych. Ponadto – pod warunkiem że spełnione są warunki określone w niniejszym rozporządzeniu –możliwość dzielenia się danymi do celów prowadzenia badań lub opracowywania, tworzenia i rozpowszechniania statystyki publicznej nie powinna być ograniczona. Organy sektora publicznego powinny również mieć możliwość wymiany danych pozyskanych na podstawie niniejszego rozporządzenia z innymi organami sektora publicznego, Komisją, Europejskim Bankiem Centralnym lub organami Unii, aby odpowiedzieć na wyjątkowe potrzeby, w związku z którymi wystąpiono z wnioskiem o dane.

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

(71) Posiadacze danych powinni móc odrzucić wniosek, z którym wystąpiły organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii albo zwrócić się o jego zmianę bez zbędnej zwłoki i w każdym przypadku nie później niż w terminie 5 lub 30 dni roboczych w zależności od charakteru wyjątkowej potrzeby, na którą powołano się we wniosku. W stosownych przypadkach posiadacz danych powinien mieć taką możliwość, jeżeli nie ma kontroli nad żądanymi danymi, tzn. jeżeli nie ma do nich natychmiastowego dostępu i nie może stwierdzić ich dostępności. Uzasadnionym powodem odmowy dzielenia się danymi jest wykazana okoliczność, że podobny wniosek został już wcześniej złożony w tym samym celu przez inny organ sektora publicznego, Komisję, Europejski Bank Centralny lub inny organ Unii, a posiadacz danych nie został powiadomiony o usunięciu danych zgodnie z niniejszym rozporządzeniem.. Posiadacz danych, który odrzuca wniosek lub zwraca się o jego zmianę, powinien przedstawić stosowne uzasadnienie organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii występującym z wnioskiem o dane. Gdy do żądanych zestawów danych mają zastosowanie prawa *sui generis* do baz danych przewidziane w dyrektywie 96/9/WE Parlamentu Europejskiego i Rady[1], posiadacze danych powinni wykonywać przysługujące im prawa w sposób, który nie uniemożliwia organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii pozyskania danych lub dzielenia się nimi zgodnie z niniejszym rozporządzeniem.

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

(72) W przypadku wyjątkowej potrzeby związanej z reagowaniem na niebezpieczeństwo publiczne organy sektora publicznego powinny, o ile to możliwe, wykorzystywać dane nieosobowe. W przypadku wniosków na podstawie wyjątkowej potrzeby, ale niezwiązanych z niebezpieczeństwem publicznym, nie można wystąpić z wnioskiem o dane osobowe. Jeżeli w zakres wniosku wchodzą dane osobowe, posiadacz danych powinien zanonimizować dane. Jeżeli uwzględnienie danych osobowych w danych udostępnianych organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii jest ściśle niezbędne lub jeżeli anonimizacja danych okaże się niemożliwa, organ występujący z wnioskiem o dane powinien wykazać, że dane te są ściśle niezbędne, oraz przedstawić konkretne i ograniczone cele przetwarzania. Należy przestrzegać mających zastosowanie przepisów dotyczących ochrony danych osobowych. Udostępniając, a następnie wykorzystując dane, należy zapewnić zabezpieczenia chroniące prawa i interesy osób fizycznych, których dane te dotyczą.

(73) Dane udostępniane organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organom Unii na podstawie wyjątkowej potrzeby należy wykorzystywać wyłącznie w celu wskazanym we wniosku, chyba że posiadacz danych, który udostępnił dane, udzielił wyraźnej zgody na wykorzystanie tych danych do innych celów. Dane należy usunąć, gdy tylko przestaną być niezbędne do celu wskazanego we wniosku, chyba że uzgodniono inaczej, a o ich usunięciu należy powiadomić posiadacza danych. Niniejsze rozporządzenie opiera się na systemach dostępu obowiązujących w Unii i w państwach członkowskich i nie zmienia prawa krajowego dotyczącego dostępu do dokumentów w kontekście obowiązków dotyczących przejrzystości. Dane należy usunąć, gdy tylko przestaną być potrzebne do wywiązania się z takich obowiązków dotyczących przejrzystości.

(74) Ponownie wykorzystując dane dostarczone przez posiadaczy danych, organy sektora publicznego, Komisja, Europejski Bank Centralny lub organy Unii powinny przestrzegać zarówno mającego zastosowanie prawa Unii lub prawa krajowego, jak i zobowiązań umownych, którym podlega posiadacz danych. Powinny one powstrzymać się od opracowania lub udoskonalenia produktu skomunikowanego lub usługi powiązanej, które konkurują z produktem skomunikowanym lub usługą powiązaną posiadacza danych, oraz od dzielenia się danymi w tych celach z osobą trzecią. Powinny one także na wniosek posiadaczy danych zapewnić im publiczne uznanie i powinny być odpowiedzialne za utrzymanie bezpieczeństwa otrzymanych danych. W przypadku gdy ujawnienie tajemnic przedsiębiorstwa posiadacza danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organom Unii jest ściśle niezbędne do osiągnięcia celu wskazanego we wniosku o dane, przed ujawnieniem danych należy zagwarantować poufność takiego ujawnienia.

(75) Jeżeli konieczna jest ochrona istotnego dobra publicznego, np. w przypadku reagowania na niebezpieczeństwa publiczne, od danego organu sektora publicznego, Komisji, Europejskiego Banku Centralnego lub organu Unii nie należy oczekiwać wypłaty przedsiębiorstwom rekompensaty za pozyskane dane. Niebezpieczeństwo publiczne należy do zdarzeń rzadkich i nie wszystkie przypadki takiego niebezpieczeństwa wymagają wykorzystywania danych będących w posiadaniu przedsiębiorstw. Jednocześnie obowiązek dostarczenia danych może stanowić znaczne obciążenie dla mikroprzedsiębiorstw i małych przedsiębiorstw. Powinny więc one móc domagać się rekompensaty nawet w kontekście reagowania na niebezpieczeństwo publiczne. Korzystanie z przepisów niniejszego rozporządzenia przez organy sektora publicznego, Komisję, Europejski Bank Centralny lub organy Unii prawdopodobnie nie będzie więc negatywnie wpływać na działalność gospodarczą posiadaczy danych. Ponieważ jednak częściej mogą występować przypadki wyjątkowej potrzeby niezwiązane z reagowaniem na niebezpieczeństwo publiczne, w takich przypadkach posiadacze danych powinni być uprawnieni do zasadnej rekompensaty, której kwota nie powinna przekraczać kosztów technicznych i organizacyjnych poniesionych w związku z zastosowaniem się do wniosku i stosownej marży żądanej za udostępnienie danych organowi sektora publicznego, Komisji, Europejskiego Banku Centralnego lub organowi Unii. Rekompensaty nie należy rozumieć jako płatności za same dane i jako płatności obowiązkowej. Posiadacze danych nie powinni móc domagać się rekompensaty, w przypadku gdy prawo krajowe nie zezwala krajowym urzędom statystycznym lub innym organom krajowym odpowiedzialnym za tworzenie statystyk na wynagradzanie posiadaczy danych za ich udostępnienie. Dany organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii powinny móc zakwestionować poziom rekompensaty żądanej przez posiadacza danych poprzez wniesienie sprawy do właściwego organu państwa członkowskiego, w którym siedzibę ma posiadacz danych.

(76) Organ sektora publicznego lub Komisja, Europejski Bank Centralny lub organ Unii powinny móc dzielić się danymi pozyskanymi na podstawie wniosku z innymi podmiotami lub osobami, jeżeli jest to niezbędne dla prowadzenia działań naukowych lub analitycznych, których nie są w stanie przeprowadzić samodzielnie, pod warunkiem że działania te są zgodne z celem, w którym wystąpiono o dane. Powinny one w odpowiednim czasie informować posiadacza danych o takim dzieleniu się danymi. Takimi danymi można również dzielić się w takich samych okolicznościach z krajowymi urzędami statystycznymi i Eurostatem do celów opracowywania, tworzenia i rozpowszechniania statystyki publicznej. Takie działania naukowe powinny jednak być zgodne z celem, w którym wystąpiono o dane, a posiadacza danych należy powiadomić o dalszym dzieleniu się danymi, których dostarczył. Osoby fizyczne prowadzące badania lub organizacje badawcze, z którymi można dzielić się tymi danymi, powinny prowadzić działalność o charakterze niekomercyjnym albo prowadzić działalność w interesie publicznym uznanym przez państwo. Do celów niniejszego rozporządzenia za organizacje badawcze nie uznaje się organizacji znajdujących się pod znacznym wpływem przedsiębiorstw komercyjnych, które mogą sprawować kontrolę nad daną organizacją z powodu okoliczności strukturalnych, przez co może dochodzić do udzielania preferencyjnego dostępu do wyników badań.

(77) Aby można było poradzić sobie z transgranicznym niebezpieczeństwem publicznym lub inną wyjątkową potrzebą, wnioski o dane mogą być kierowane do posiadaczy danych w państwach członkowskich innych niż państwo występującego z wnioskiem organu sektora publicznego. W takim przypadku organ sektora publicznego powinien poinformować właściwy organ państwa członkowskiego, w którym posiadacz danych ma siedzibę, tak by organ ten mógł sprawdzić wniosek pod kątem kryteriów ustanowionych w niniejszym rozporządzeniu. To samo powinno mieć zastosowanie do wniosków Komisji, Europejskiego Banku Centralnego lub organu Unii. Jeżeli wystąpiono z wnioskiem o dane osobowe, organ sektora publicznego powinien poinformować o tym organ nadzorczy odpowiedzialny za monitorowanie stosowania rozporządzenia (UE) 2016/679 w państwie członkowskim, w którym organ sektora publicznego ma siedzibę. Dany właściwy organ powinien być uprawniony do doradzania organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii, by podjęli oni współpracę z organem sektora publicznego w państwie członkowskim, w którym posiadacz danych ma siedzibę, w celu zapewnienia jak najmniejszego obciążenia administracyjnego dla posiadacza danych. W przypadku gdy właściwy organ zgłosi uzasadniony sprzeciw co do zgodności wniosku z niniejszym rozporządzeniem, powinien on odrzucić wniosek organu sektora publicznego, Komisji, Europejskiego Banku Centralnego, które z kolei powinny uwzględnić ten sprzeciw przed podjęciem dalszego działania, w tym ponownego wystąpienia z wnioskiem.

(78) Podstawowym warunkiem, który pozwoli stworzyć bardziej konkurencyjny rynek, charakteryzujący się mniejszymi barierami wejścia dla nowych dostawców usług przetwarzania danych, oraz zapewnić użytkownikom tych usług większą odporność, jest umożliwienie klientom korzystającym z usług przetwarzania danych, w tym usług w chmurze i usług przetwarzania brzegowego, zmiany dostawcy usługi przetwarzania danych z zachowaniem minimalnego poziomu funkcjonalności usługi i bez przestoju usług lub umożliwienie korzystania z usług kilku dostawców jednocześnie bez nieuzasadnionych przeszkód i kosztów przekazywania danych. Z przepisów dotyczących zmiany dostawcy ustanowionych w niniejszym rozporządzeniu powinni korzystać też klienci korzystający z ofert bezpłatnych, tak by oferty te nie skutkowały dla nich uzależnieniem od jednego dostawcy.

(79) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807[1] zachęca dostawców usług przetwarzania danych do opracowywania i skutecznego wdrażania samoregulacyjnych kodeksów postępowania, obejmujących m.in. najlepsze praktyki w zakresie ułatwiania zmiany dostawców usług przetwarzania danych i w zakresie przenoszenia danych. Mając na uwadze ograniczone korzystanie z ram samoregulacyjnych opracowanych w związku z tym rozporządzeniem, oraz ogólną niedostępność otwartych standardów i interfejsów, należy przyjąć zestaw minimalnych obowiązków regulacyjnych, które będą spoczywać na dostawcach usług przetwarzania danych, w celu wyeliminowania przeszkód przedkomercyjnych, komercyjnych, technicznych, umownych i organizacyjnych, które nie ograniczają się do zmniejszonej szybkości transferu danych przy odejściu klienta, i które utrudniają skuteczną zmianę dostawcy usług przetwarzania danych.

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.U. L 303 z 28.11.2018, s. 59).

(80) Usługi przetwarzania danych powinny obejmować usługi umożliwiające wszechobecny sieciowy dostęp na żądanie do konfigurowalnego, skalowalnego i elastycznego wspólnego zbioru rozproszonych zasobów obliczeniowych. Zasoby obliczeniowe obejmują takie zasoby jak sieci, serwery lub inną infrastrukturę wirtualną lub fizyczną, oprogramowanie, w tym narzędzia do tworzenia oprogramowania, pamięć masową, aplikacje i usługi. Zdolność klienta korzystającego z usługi przetwarzania danych do jednostronnego zapewnienia sobie możliwości obliczeniowych, takich jak czas serwera lub pamięć sieciowa, bez ingerencji ludzkiej ze strony dostawcy usług przetwarzania danych, można określić jako wymagającą minimalnego wysiłku pod względem zarządzania i związaną z minimalną interakcją między dostawcą a klientem. Pojęcia „wszechobecne" używa się do opisu sytuacji, w której możliwości obliczeniowe są udostępniane przez sieć, a dostęp do nich jest możliwy za pośrednictwem mechanizmów sprzyjających wykorzystywaniu różnorodnych platform cienkich lub grubych klientów (od przeglądarek internetowych po urządzenia mobilne i stacje robocze). Pojęcie „skalowalne" odnosi się do zasobów obliczeniowych, które są elastycznie przydzielane przez dostawcę usług przetwarzania danych, niezależnie od położenia geograficznego zasobów, jako reakcja na zmiany zapotrzebowania. Pojęcia „elastyczne " używa się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie od zapotrzebowania, aby szybko zwiększać lub zmniejszać dostępne zasoby w zależności od obciążenia. Pojęcia „wspólny zbiór" używa się do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, jednak przetwarzanie odbywa się oddzielnie dla każdego z użytkowników, choć usługa ta jest świadczona z tego samego sprzętu elektronicznego. Pojęcia „rozproszone" używa się do opisu zasobów obliczeniowych zlokalizowanych na rożnych komputerach lub urządzeniach połączonych w sieć, które komunikują się ze sobą i koordynują swoją pracę przez przekazywanie komunikatów. Pojęcia „wysoce rozproszone" używa się do opisu usług przetwarzania danych, które obejmują przetwarzanie danych prowadzone w bliższej odległości do miejsca generowania lub zbierania danych, np. w skomunikowanym urządzeniu do przetwarzania danych. Oczekuje się, że przetwarzanie brzegowe, które stanowi rodzaj takiego wysoce rozproszonego przetwarzania danych, spowoduje rozwój nowych modeli biznesowych i modeli świadczenia usług w chmurze, które od początku powinny być otwarte i interoperacyjne.

(81) Ogólne pojęcie „usługi przetwarzania danych” obejmuje znaczną liczbę usług o bardzo szerokich i różnorodnych celach, funkcjach i konfiguracjach technicznych. W powszechnym rozumieniu dostawców i użytkowników oraz zgodnie z powszechnie stosowanymi normami usługi przetwarzania danych należą do co najmniej jednego z następujących trzech modeli świadczenia usług przetwarzania danych: infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) i oprogramowanie jako usługa (SaaS). Te modele świadczenia usług stanowią konkretne gotowe pakiety zasobów technologii informacyjno-komunikacyjnych (ICT) oferowane przez dostawcę usług przetwarzania danych. Te trzy podstawowe modele świadczenia usług przetwarzania danych są dodatkowo uzupełnione nowymi opcjami, z których każda jest innym pakietem zasobów ICT, takimi jak StaaS (przechowywanie jako usługa) i DBaaS (baza danych jako usługa). Usługi przetwarzania danych można skategoryzować w bardziej szczegółowy sposób i podzielić na niewyczerpującą listę zestawów usług przetwarzania danych, które mają ten sam główny cel i te same główne funkcje oraz opierają się na tym samym rodzaju modeli przetwarzania danych, niezwiązanych z charakterystyką operacyjną usługi (zwaną dalej „usługą tego samego typu”). Usługi należące do tego samego typu mogą posługiwać się takim samym modelem usługi przetwarzania danych, jednak dwie bazy danych mogą pozornie mieć ten sam główny cel, ale po przyjrzeniu się ich modelowi przetwarzania danych, modelowi dystrybucji i założonym sposobom wykorzystywania można by je przypisać do bardziej szczegółowej podkategorii usług podobnych. Usługi tego samego typu mogą mieć odmienne i konkurencyjne cechy, takie jak wydajność, bezpieczeństwo, odporność i jakość usług.

(82) Stwarzanie trudności w ekstrakcji danych eksportowalnych należących do klienta wyjściowego dostawcy usług przetwarzania danych może być przeszkodą w przywracaniu funkcji usługi w infrastrukturze docelowego dostawcy usług przetwarzania danych. Aby ułatwić klientowi strategię odejścia, zapobiec zbędnym i uciążliwym zadaniom oraz zapewnić, by w wyniku procesu zmiany dostawcy klient nie stracił żadnych swoich danych, wyjściowy dostawca usług przetwarzania danych powinien z wyprzedzeniem poinformować klienta o zakresie danych, które można wyeksportować, gdy klient podejmie decyzję o zmianie dostawcy usługi przetwarzania danych lub o przejściu na lokalną infrastrukturę ICT. Zakres danych eksportowalnych powinien obejmować co najmniej dane wejściowe i wyjściowe, w tym metadane, bezpośrednio lub pośrednio wygenerowane bądź współwygenerowane w wyniku korzystania przez klienta z usługi przetwarzania danych, z wyłączeniem wszelkich aktywów lub danych dostawcy usług przetwarzania danych lub osoby trzeciej. Z danych eksportowalnych należy wyłączyć wszelkie dane dostawcy usługi przetwarzania danych lub osób trzech, które są chronione prawami własności intelektualnej lub stanowią tajemnicę przedsiębiorstwa tego dostawcy lub tych osób trzecich, oraz dane związane z integralnością i bezpieczeństwem usługi, których eksport czyniłby dostawcę usługi przetwarzania danych podatnym na cyberzagrożenia. Wyłączenia te nie powinny utrudniać ani opóźniać procesu zmiany dostawcy.

(83) Aktywa cyfrowe oznaczają elementy w formacie cyfrowym, z których klient ma prawo korzystać, w tym aplikacje i metadane związane z konfiguracją ustawień, bezpieczeństwem oraz zarządzaniem prawami dostępu i prawami kontroli, oraz inne elementy, takie jak stanowiące wyraz technologii wirtualizacji, w tym maszyny wirtualne i kontenery. Aktywa cyfrowe mogą być przenoszone, jeżeli klient ma prawo z nich korzystać, niezależnie od stosunku umownego obejmującego usługę przetwarzania danych, w przypadku której zamierza zmienić dostawcę. Te inne elementy są nieodzowne do skutecznego wykorzystywania danych i aplikacji klienta w środowisku docelowego dostawcy usług przetwarzania danych.

(84) Niniejsze rozporządzenie ma ułatwić zmianę dostawcy usług przetwarzania danych, przy czym taka zmiana obejmuje warunki i działania niezbędne do rozwiązania przez klienta umowy dotyczącej usługi przetwarzania danych, zawarcia co najmniej jednej nowej umowy z innymi dostawcami usług przetwarzania danych, przeniesienia swoich danych eksportowalnych i aktywów cyfrowych oraz w stosownym przypadku skorzystania z równoważności funkcjonalnej.

(85) Zmiana dostawcy to operacja podejmowana z inicjatywy klienta i obejmująca kilka etapów, w tym ekstrakcję danych, przez którą rozumie się pobranie danych z ekosystemu wyjściowego dostawcy usług przetwarzania danych, transformację, w przypadku gdy dane są strukturyzowane w sposób, który nie odpowiada schematowi lokalizacji docelowej, i załadowanie danych do nowej lokalizacji docelowej. W szczególnej sytuacji opisanej w niniejszym rozporządzeniu za zmianę dostawcy należy uznać również wyłączenie danej usługi z umowy i przeniesienie jej do innego dostawcy. Procesem zmiany dostawcy zarządza niekiedy w imieniu klienta podmiot będący osobą trzecią. W związku z tym wszystkie prawa i obowiązki klienta ustanowione niniejszym rozporządzeniem, w tym obowiązek współpracy w dobrej wierze, należy rozumieć w takich okolicznościach jako mające zastosowanie do takiego podmiotu będącego osobą trzecią. Dostawcy usług przetwarzania danych i klienci mają obowiązki na różnych poziomach, w zależności od etapu procesu, o którym mowa. Na przykład wyjściowy dostawca usług przetwarzania danych jest odpowiedzialny za ekstrakcję danych do formatu nadającego się do odczytu maszynowego, ale to klient i docelowy dostawca usług przetwarzania danych ładują dane do nowego środowiska, chyba że została zamówiona konkretna profesjonalna usługa przeniesienia danych. Klient, który zamierza wykonać prawa związane ze zmianą dostawcy przewidziane w niniejszym rozporządzeniu, powinien poinformować wyjściowego dostawcę usług przetwarzania danych o decyzji, aby zmienić dostawcę usług przetwarzania danych, przejść na lokalną infrastrukturę ICT albo usunąć aktywa tego klienta i jego dane eksportowalne.

(86) Równoważność funkcjonalna oznacza przywrócenie – na podstawie danych eksportowalnych i aktywów cyfrowych klienta – minimalnego poziomu funkcjonalności danej usługi tego samego typu w środowisku nowej usługi przetwarzania danych po zmianie dostawcy, przy czym usługa docelowa przetwarzania danych daje porównywalny rezultat w reakcji na te same dane wejściowe w przypadku wspólnych cech dostarczanych klientowi na podstawie umowy. Od dostawców usług przetwarzania danych można wyłącznie oczekiwać ułatwienia równoważności funkcjonalnej dla jednakowych funkcji oferowanych niezależnie od siebie przez usługę wyjściową i usługę docelową przetwarzania danych. Niniejsze rozporządzenie nie nakłada obowiązku ułatwienia równoważności funkcjonalnej na dostawców usług przetwarzania danych innych niż dostawcy oferujący usługi w modelu IaaS.

(87) Usługi przetwarzania danych są wykorzystywane w różnych sektorach i różnią się złożonością i rodzajem. Jest to kwestia istotna z punktu widzenia procesu przenoszenia danych i ram czasowych. Jednak na przedłużenie okresu przejściowego z powodu technicznej niemożliwości finalizacji procesu zmiany dostawcy w danych ramach czasowych powinno móc się powołać wyłącznie w należycie uzasadnionych przypadkach. Ciężar dowodu w tej kwestii powinien w pełni spoczywać na danym dostawcy usługi przetwarzania danych. Pozostaje to bez uszczerbku dla wyłącznego prawa klienta do jednokrotnego przedłużenia okresu przejściowego o okres, który klient uznaje za bardziej odpowiadający jego własnym celom. Na prawo do przedłużenia okresu przejściowego klient może się powołać przed okresem przejściowym lub w trakcie okresu przejściowego, z uwzględnieniem faktu, że w okresie przejściowym nadal ma zastosowanie umowa.

(88) Opłaty z tytułu zmiany dostawcy usług przetwarzania danych to opłaty nakładane na klientów przez dostawców usług przetwarzania danych za proces zmiany dostawcy. Zwykle opłaty te mają na celu przeniesienie kosztów, które dostawca wyjściowy usług przetwarzania danych może ponieść w związku z procesem zmiany, na klienta, który chce zmienić dostawcę. Powszechnymi przykładami opłat z tytułu zmiany dostawcy są koszty związane z przemieszczeniem danych od jednego dostawcy usług przetwarzania danych do drugiego lub do lokalnej infrastruktury ICT (zwane dalej „opłatami z tytułu wychodzącego ruchu danych") lub koszty konkretnych działań wspierających podczas procesu zmiany dostawcy. Nadmiernie wysokie opłaty z tytułu wychodzącego ruchu danych i inne nieuzasadnione opłaty niezwiązane z rzeczywistymi kosztami zmiany dostawcy utrudniają klientom zmianę dostawcy, ograniczają swobodny przepływ danych, mogą ograniczać konkurencję i dają efekt uzależnienia klientów od jednego dostawcy, gdyż zmniejszają motywację do wyboru innego lub dodatkowego dostawcy usług. W związku z tym opłaty z tytułu zmiany dostawcy powinny zostać zniesione po trzech latach od dnia wejścia w życie niniejszego rozporządzenia. Dostawcy usług przetwarzania danych powinni mieć możliwość nakładania do tego dnia obniżonych opłat za zmianę dostawcy.

(89) Wyjściowy dostawca usług przetwarzania danych powinien mieć możliwość zlecania niektórych zadań na zasadzie outsourcingu i wypłacania rekompensaty podmiotom będącym osobą trzecią w celu wypełnienia obowiązków przewidzianych w niniejszym rozporządzeniu. Klient nie powinien ponosić kosztów wynikających ze zlecenia usług na zasadzie outsourcingu przez dostawcę usług przetwarzania danych podczas procesu zmiany dostawcy, a koszty takie należy uznać za nieuzasadnione, chyba że koszty te dotyczą prac podjętych przez dostawcę usług przetwarzania danych na wniosek klienta w zakresie dodatkowego wsparcia w procesie zmiany dostawcy, a prace te wykraczają poza obowiązki dostawcy w ramach zmiany dostawcy wyraźnie przewidziane w niniejszym rozporządzeniu. Niniejsze rozporządzenie nie uniemożliwia klientowi wypłacania rekompensaty podmiotom będącym osobą trzecią za wsparcie w procesie migracji ani nie uniemożliwia stronom uzgadniania umów na czas określony w sprawie usług przetwarzania danych, w tym proporcjonalnych kar za wcześniejsze rozwiązanie tej umowy, zgodnie z prawem Unii lub prawem krajowym. Aby sprzyjać konkurencji, stopniowe wycofywanie opłat związanych ze zmianą dostawcy usług przetwarzania danych powinno obejmować w szczególności opłaty z tytułu wychodzącego ruchu danych nakładane na klienta przez dostawcę usług przetwarzania danych. Standardowe opłaty za usługę w zamian za świadczenie usług przetwarzania danych same w sobie nie są opłatami za zmianę dostawcy. Standardowe opłaty za usługę nie podlegają wycofaniu i nadal mają zastosowanie, do czasu aż przestanie obowiązywać umowa świadczenia danych usług. Niniejsze rozporządzenie umożliwia klientowi występowanie z wnioskiem o świadczenie dodatkowych usług wykraczających poza obowiązki spoczywające na dostawcy w ramach zmiany dostawcy na podstawie niniejszego rozporządzenia. Te dodatkowe usługi mogą być wykonywane przez dostawcę i może on pobierać za nie opłaty, jeżeli usługi są wykonywane na wniosek klienta, a klient uprzednio zgodził się z ich wyceną.

(90) Potrzebne jest ambitne i zachęcające do innowacji podejście regulacyjne do interoperacyjności, aby przezwyciężyć uzależnienie od jednego dostawcy, które osłabia konkurencję i opracowywanie nowych usług. Interoperacyjność między usługami przetwarzania danych obejmuje liczne interfejsy oraz warstwy infrastruktury i oprogramowania i rzadko ogranicza się do testu, czy jest osiągalna, czy nie. Wręcz przeciwnie, tworzenie takiej interoperacyjności podlega analizie kosztów i korzyści, która jest niezbędna do ustalenia, czy warto dążyć do racjonalnie przewidywalnych wyników. Ważnym punktem odniesienia w kontekście realizacji celów niniejszego rozporządzenia jest międzynarodowa norma ISO/IEC 19941:2017, która obejmuje aspekty techniczne wyjaśniające złożoność takiego procesu.

(91) W przypadku gdy dostawcy usług przetwarzania danych są z kolei klientami korzystającymi z usług przetwarzania danych świadczonych przez dostawcę będącego osobą trzecią, sami odniosą korzyść ze skuteczniejszej możliwości zmiany dostawcy, a jednocześnie będą nadal podlegać obowiązkom określonym w niniejszym rozporządzeniu w odniesieniu do własnej oferty usług.

(92) Dostawcy usług przetwarzania danych powinni być zobowiązani do oferowania w ramach swoich kompetencji, proporcjonalnie do swoich obowiązków, wszelkiej pomocy i wszelkiego wsparcia, które są potrzebne, aby proces zmiany dostawcy na innego dostawcę usług przetwarzania danych był udany, skuteczny i bezpieczny. Niniejsze rozporządzenie nie zobowiązuje dostawców usług przetwarzania danych do opracowania nowych kategorii usług przetwarzania danych, w tym w ramach infrastruktury ICT innych dostawców usług przetwarzania danych lub na podstawie takiej infrastruktury, w celu zagwarantowania równoważności funkcjonalnej w środowisku innym niż własne systemy. Wyjściowy dostawca usług przetwarzania danych nie ma dostępu do środowiska docelowego dostawcy usług przetwarzania danych ani wglądu w to środowisko. Nie należy rozumieć, że równoważność funkcjonalna zobowiązuje wyjściowego dostawcę usług przetwarzania danych do odtworzenia danej usługi w ramach infrastruktury docelowego dostawcy usług przetwarzania danych. Wyjściowy dostawca usług przetwarzania danych powinien natomiast podjąć w granicach swoich uprawnień wszelkie rozsądne działania, aby ułatwić osiągnięcie równoważności funkcjonalnej, zapewniając zdolności, odpowiednie informacje, dokumentację, wsparcie techniczne oraz w stosownym przypadku niezbędne narzędzia.

(93) Dostawcy usług przetwarzania danych powinni także być zobowiązani do usunięcia istniejących przeszkód i do nienakładania nowych, w tym wobec klientów chcących przejść na lokalną infrastrukturę ICT. Przeszkody mogą m.in. mieć charakter przedkomercyjny, komercyjny, techniczny, umowny lub organizacyjny. Dostawcy usług przetwarzania danych powinni także być zobowiązani do usunięcia przeszkód w oddzieleniu konkretnej usługi od innych przewidzianych w umowie usług przetwarzania danych i do udostępnienia odpowiedniej usługi w celu zmiany dostawcy, o ile nie istnieją duże i możliwe do wykazania przeszkody techniczne uniemożliwiające takie oddzielenie.

(94) Podczas całego procesu zmiany dostawcy należy zachować wysoki poziom bezpieczeństwa. Oznacza to, że wyjściowy dostawca usług przetwarzania danych powinien objąć poziomem bezpieczeństwa, do którego jest zobowiązany w ramach usługi, wszystkie uzgodnienia techniczne, za które odpowiada podczas procesu zmiany dostawcy, takie jak połączenia sieciowe czy urządzenia fizyczne. Nie należy spodziewać się wpływu na obowiązujące prawa dotyczące rozwiązywania umów, w tym prawa wprowadzone rozporządzeniem (UE) 2016/679 i dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/770[1]. Nie należy rozumieć, że niniejsze rozporządzenie stoi na przeszkodzie temu, by dostawca usług przetwarzania danych zapewniał swoim klientom nowe i udoskonalone usługi, cechy czy funkcje, ani temu, by konkurował na tej podstawie z innymi dostawcami usług przetwarzania danych.

---

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.U. L 136 z 22.5.2019, s. 1).

(95) Informacje, które dostawca usług przetwarzania danych ma przedstawić klientowi, mogą być wsparciem w strategii odejścia klienta. Informacje te powinny obejmować procedury inicjowania zmiany dostawcy usługi przetwarzania danych, formaty danych nadające się do odczytu maszynowego, do których mogą być wyeksportowane dane użytkownika, narzędzia przeznaczone do eksportowania danych, w tym otwarte interfejsy oraz informacje o zgodności z normami zharmonizowanymi lub wspólnymi specyfikacjami opartymi na otwartych specyfikacjach w zakresie interoperacyjności; informacje o znanych ograniczeniach technicznych, które mogą wpłynąć na proces zmiany dostawcy, a także szacowany czas niezbędny do zakończenia procesu zmiany dostawcy.

(96) Aby ułatwić interoperacyjność i zmianę dostawcy usług przetwarzania danych, użytkownicy i dostawcy usług przetwarzania danych powinni rozważyć korzystanie z narzędzi wdrażania lub zapewniania zgodności, w szczególności narzędzi publikowanych przez Komisję w postaci unijnego zbioru przepisów dotyczących chmury obliczeniowej i wytycznych dotyczących zamówień publicznych na usługi przetwarzania danych. Wzrostowi wiarygodności usług przetwarzania danych, tworzeniu bardziej wyważonych stosunków między użytkownikami a dostawcami usług przetwarzania danych oraz większej pewności prawa w kwestii warunków mających zastosowanie do zmiany dostawcy usług przetwarzania danych sprzyjają w szczególności standardowe postanowienia umowne. W związku z tym użytkownicy i dostawcy usług przetwarzania danych powinni rozważyć posługiwanie się standardowymi postanowieniami umownymi – lub innymi samoregulacyjnymi narzędziami zapewniania zgodności, o ile w pełni spełniają one wymagania niniejszego rozporządzenia – opracowanymi przez stosowne organy lub grupy ekspertów ustanowione na mocy prawa Unii.

(97) Aby ułatwić zmianę dostawcy usług przetwarzania danych, wszystkie zaangażowane strony, w tym dostawcy wyjściowi i docelowi usług przetwarzania danych, powinny współpracować w dobrej wierze, tak aby umożliwić pomyślny proces zmiany dostawcy oraz bezpieczne i terminowe przekazanie niezbędnych danych w powszechnie używanym formacie nadającym się do odczytu maszynowego i za pomocą otwartego interfejsu, a przy tym nie dopuścić do zakłóceń w świadczeniu usługi i utrzymać jej ciągłość.

(98) Usługi przetwarzania danych, w przypadku których większość głównych cech została opracowana na zamówienie, tak aby dostosować je do konkretnych żądań indywidualnego klienta, lub w przypadku których wszystkie komponenty zostały opracowane na potrzeby indywidualnego klienta, powinny być zwolnione z niektórych obowiązków mających zastosowanie do zmiany dostawcy usług przetwarzania danych. Nie powinno to dotyczyć usług, które dostawca usług przetwarzania danych oferuje komercyjnie na szeroką skalę poprzez katalog usług. Jednym z obowiązków dostawcy usług przetwarzania danych jest należyte poinformowanie przyszłych klientów mających korzystać z takich usług przed zawarciem umowy o obowiązkach określonych w niniejszym rozporządzeniu, które nie mają zastosowania do danych usług. Nic nie stoi na przeszkodzie, aby dostawca usług ostatecznie wprowadził takie usługi na dużą skalę, w którym to przypadku musiałby wywiązywać się ze wszystkich obowiązków związanych ze zmianą dostawcy określonych w niniejszym rozporządzeniu.

(99) Zgodnie z minimalnym wymaganiem, którym jest umożliwienie zmiany dostawcy usług przetwarzania danych, niniejsze rozporządzenie ma na celu także zwiększenie interoperacyjności na potrzeby równoczesnego korzystania z wielu usług przetwarzania danych o komplementarnych funkcjach. Dotyczy to sytuacji, w których klienci nie rozwiązują umów, aby zmienić dostawcę przetwarzania danych, ale w których w sposób interoperacyjny korzysta się równocześnie z wielu usług różnych dostawców, aby móc posługiwać się komplementarnymi funkcjami tych usług w ramach konfiguracji systemu klienta. Uznaje się jednak, że wychodzący ruch danych od jednego dostawcy usług przetwarzania danych do innego, aby ułatwić równoczesne korzystanie z usług, może być zdarzeniem ciągłym, w przeciwieństwie do jednorazowego ruchu wychodzącego wymaganego w ramach procesu zmiany dostawcy. Dostawcy usług przetwarzania danych powinni zatem mieć nadal możliwość nakładania opłat, nieprzekraczających poniesionych kosztów, z tytułu wychodzącego ruchu danych do celów równoczesnego korzystania z usług, po upływie trzech lat od dnia wejścia w życie niniejszego rozporządzenia ale nieprzekraczające poniesionych kosztów. Jest to istotne m.in. dla skutecznej realizacji strategii wielochmurowych, które umożliwiają klientom wdrażanie przyszłościowych strategii ICT i zmniejszają zależność od pojedynczych dostawców usług przetwarzania danych. Ułatwienie podejścia wielochmurowego w przypadku klientów usług przetwarzania danych może również przyczynić się do zwiększenia ich operacyjnej odporności cyfrowej, co zostało uznane w odniesieniu do instytucji świadczących usługi finansowe w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554[1].

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2002, s. 1).

(100) Otwarte specyfikacje i normy w zakresie interoperacyjności opracowane zgodnie z załącznikiem II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012[1] w obszarze interoperacyjności i przenoszenia mają umożliwiać tworzenie środowiska chmury obliczeniowej bazującego na usługach świadczonych przez wielu dostawców, co stanowi kluczowe wymaganie w kontekście otwartych innowacji w europejskiej gospodarce opartej na danych. Ponieważ rozpowszechnienie na rynku norm zidentyfikowanych w ramach zakończonej w 2016 r. inicjatywy dotyczącej koordynacji normalizacji w chmurze (CSC) było ograniczone, konieczne jest, by Komisja również polegała na stronach działających na rynku w zakresie opracowywania stosownych otwartych specyfikacji w zakresie interoperacyjności, aby nadążyć za szybkim tempem rozwoju technologicznego w tej branży. Takie otwarte specyfikacje w zakresie interoperacyjności Komisja może następnie przyjąć w formie wspólnych specyfikacji. Ponadto w przypadku gdy nie wykazano, aby procesy rynkowe mogły skutkować ustanowieniem wspólnych specyfikacji lub norm ułatwiających zapewnienie skutecznej interoperacyjności usług w chmurze na poziomie PaaS i SaaS, Komisja – na podstawie niniejszego rozporządzenia i zgodnie z rozporządzeniem (UE) nr 1025/2012 – powinna móc wystąpić do europejskich organizacji normalizacyjnych z wnioskiem o opracowanie takich norm dla określonych typów usług, jeżeli takie normy jeszcze nie istnieją. Ponadto Komisja będzie zachęcać strony działające na rynku do opracowania stosownych otwartych specyfikacji w zakresie interoperacyjności.

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

Po konsultacjach z zainteresowanymi stronami Komisja powinna móc – w drodze aktów wykonawczych – nakazać stosowanie zharmonizowanych norm interoperacyjności lub wspólnych specyfikacji w zakresie interoperacyjności dla określonych typów usług poprzez odniesienie do nich w centralnym repozytorium norm Unii dotyczących interoperacyjności usług przetwarzania danych. Dostawcy usług przetwarzania danych powinni zapewnić przestrzeganie tych zharmonizowanych norm i wspólnych specyfikacji opartych na otwartych specyfikacjach w zakresie interoperacyjności, to zaś nie powinno negatywnie wpływać na bezpieczeństwo lub integralność danych. Odniesienie do zharmonizowanych norm interoperacyjności usług przetwarzania danych oraz wspólnych specyfikacji opartych na otwartych specyfikacjach w zakresie interoperacyjności zostanie poczynione wyłącznie wtedy, gdy będą one zgodne z kryteriami określonymi w niniejszym rozporządzeniu, które mają takie samo znaczenie jak wymagania określone w załączniku II do rozporządzenia (UE) nr 1025/2012 i jak aspekty interoperacyjności określone w międzynarodowej normie ISO/IEC 19941:2017. Ponadto w ramach normalizacji należy uwzględnić potrzeby MŚP.

(101) Państwa trzecie mogą przyjmować przepisy ustawowe i wykonawcze oraz inne akty prawne, których celem jest bezpośrednie przekazywanie danych nieosobowych znajdujących się poza ich granicami, w tym w Unii, lub zapewnianie administracji rządowej dostępu do takich danych. Wyroki sądów lub trybunałów czy decyzje innych organów sądowych lub administracyjnych, w tym organów ścigania, w państwach trzecich nakazujące przekazać dane nieosobowe lub zapewnić dostęp do nich powinny być wykonalne, jeżeli mają za podstawę umowę międzynarodową, np. traktat o pomocy prawnej, obowiązującą między państwem trzecim występującym z wnioskiem a Unią lub państwem członkowskim. W innych przypadkach mogą zdarzyć się sytuacje, w których wniosek o przekazanie danych nieosobowych lub zapewnienie dostępu do nich wynikający z prawa państwa trzeciego pozostaje w konflikcie z obowiązkiem ochrony takich danych wynikającym z prawa Unii lub prawa krajowego danego państwa członkowskiego, w szczególności jeśli chodzi o ochronę praw podstawowych jednostki, takich jak prawo do bezpieczeństwa i prawo do skutecznego środka prawnego, lub podstawowych interesów państwa członkowskiego związanych z bezpieczeństwem narodowym lub obroną, oraz ochronę szczególnie chronionych danych handlowych, w tym ochronę tajemnic przedsiębiorstwa, i ochronę praw własności intelektualnej, w tym z zobowiązaniami umownymi tego państwa dotyczącymi poufności zgodnie z takim prawem.
W przypadku braku umów międzynarodowych regulujących takie kwestie przekazanie lub dostęp do danych nieosobowych powinny być dozwolone wyłącznie wtedy, gdy sprawdzono, że system prawny państwa trzeciego wymaga określenia powodów i proporcjonalności decyzji, że orzeczenie sądu lub decyzja mają szczególny charakter oraz że uzasadniony sprzeciw adresata podlega kontroli właściwego sądu lub trybunału państwa trzeciego, który jest upoważniony do należytego uwzględnienia stosownych interesów prawnych dostawcy takich danych. Wszędzie tam, gdzie jest to możliwe na mocy warunków wniosku o dostęp do danych złożonego przez organ państwa trzeciego, dostawca usług przetwarzania danych powinien móc przedstawić informacje klientowi, którego dane są przedmiotem wniosku, przed udzieleniem dostępu do tych danych, w celu sprawdzenia, czy istnieje potencjalna kolizja takiego dostępu z prawem Unii lub prawem krajowym, takim jak prawo dotyczące ochrony szczególnie chronionych danych handlowych, w tym ochrony tajemnic przedsiębiorstwa i praw własności intelektualnej oraz zobowiązań umownych dotyczących poufności.

(102) Aby zwiększyć wiarygodność danych, należy w miarę możliwości wdrożyć w odniesieniu do obywateli Unii, organów sektora publicznego i przedsiębiorstw zabezpieczenia zapewniające kontrolę nad ich danymi. Ponadto należy przestrzegać prawa, wartości i norm Unii w zakresie m.in. bezpieczeństwa, ochrony danych i prywatności oraz ochrony konsumentów. Aby zapobiec niezgodnemu z prawem dostępowi administracji rządowej państwa trzeciego do danych nieosobowych, dostawcy usług przetwarzania danych podlegających niniejszemu rozporządzeniu, takich jak usługi w chmurze i usługi przetwarzania brzegowego, powinni zastosować wszelkie rozsądne środki w celu uniemożliwienia dostępu do systemów, w których przechowywane są dane nieosobowe, w tym w stosownym przypadku poprzez szyfrowanie danych, częste poddawanie się audytom, zweryfikowane przestrzeganie odpowiednich systemów certyfikacji gwarancji bezpieczeństwa oraz zmianę polityki korporacyjnej.

(103) Normalizacja i interoperacyjność semantyczna powinny odgrywać kluczową rolę w dostarczaniu rozwiązań technicznych zapewniających interoperacyjność w ramach wspólnych europejskich przestrzeni danych i pomiędzy nimi, które to przestrzenie są interoperacyjnymi ramami wspólnych norm i praktyk, specyficznymi dla danego celu lub sektora bądź międzysektorowymi, i w których ma miejsce dzielenie się danymi lub ich wspólne przetwarzanie na potrzeby m.in. opracowywania nowych produktów i usług, badań naukowych lub inicjatyw społeczeństwa obywatelskiego. Niniejsze rozporządzenie ustanawia pewne zasadnicze wymagania w dziedzinie interoperacyjności. Wymagań tych powinni przestrzegać – o ile dotyczy to elementów pozostających pod ich kontrolą – uczestnicy przestrzeni danych oferujący innym uczestnikom dane lub usługi oparte na danych i będący podmiotami ułatwiającymi dzielenie się danymi lub zaangażowanymi w dzielenie się danymi we wspólnych europejskich przestrzeniach danych, w tym posiadacze danych. Przestrzeganie tych zasad można zapewnić dzięki dostosowaniu się do zasadniczych wymagań ustanowionych w niniejszym rozporządzeniu lub można go domniemywać dzięki przestrzeganiu zharmonizowanych norm lub wspólnych specyfikacji poprzez domniemanie zgodności. W celu ułatwienia przestrzegania wymagań interoperacyjności należy przewidzieć domniemanie zgodności rozwiązań interoperacyjnych spełniających normy zharmonizowane lub ich części zgodnie z rozporządzeniem (UE) nr 1025/2012, które stanowi domyślne ramy opracowywania norm przewidujących takie domniemanie. Komisja powinna ocenić bariery dla interoperacyjności i określić priorytetowe potrzeby normalizacji, na podstawie których może wystąpić z wnioskiem do co najmniej jednej europejskiej organizacji normalizacyjnej, zgodnie z rozporządzeniem (UE) nr 1025/2012, o opracowanie norm zharmonizowanych spełniających zasadnicze wymagania określone w niniejszym rozporządzeniu.

Jeżeli takie wnioski nie poskutkują normami zharmonizowanymi lub takie normy zharmonizowane będą niewystarczające, aby zapewnić przestrzeganie zasadniczych wymagań określonych w niniejszym rozporządzeniu, Komisja powinna móc przyjąć wspólne specyfikacje w tych dziedzinach – pod warunkiem że zrobi to z należytym poszanowaniem roli i funkcji organizacji normalizacyjnych. Przyjęcie wspólnych specyfikacji powinno być wyjątkowym rozwiązaniem awaryjnym ułatwiającym przestrzeganie zasadniczych wymagań ustanowionych w niniejszym rozporządzeniu, w przypadku gdy proces normalizacji jest zablokowany lub istnieją opóźnienia w ustanawianiu odpowiednich norm zharmonizowanych. Jeżeli takie opóźnienie wynika ze złożoności technicznej danej normy, Komisja powinna wziąć tę kwestię pod uwagę, zanim rozpocznie analizę dotyczącą ustanowienia wspólnych specyfikacji. Wspólne specyfikacje powinny zostać opracowane w sposób otwarty i inkluzywny i w stosownym przypadku uwzględniać opinie przyjęte przez Europejską Radę ds. Innowacji w zakresie Danych ustanowioną na mocy rozporządzenia (UE) 2022/868. Ponadto można przyjmować wspólne specyfikacje w poszczególnych sektorach, zgodnie z prawem Unii lub prawem krajowym, na podstawie szczególnych potrzeb tych sektorów. Ponadto Komisja powinna mieć możliwość zlecić opracowanie zharmonizowanych norm interoperacyjności usług przetwarzania danych.

(104) Aby promować interoperacyjność narzędzi do automatycznego wykonywania umów o dzielenie się danymi, należy ustanowić zasadnicze wymagania dotyczące inteligentnych umów, które specjaliści tworzą dla innych lub włączają do aplikacji wspierających realizację umów o dzielenie się danymi. Aby ułatwić zapewnienie zgodności takich inteligentnych umów z tymi zasadniczymi wymaganiami, należy przewidzieć domniemanie zgodności inteligentnych umów spełniających normy zharmonizowane lub ich części zgodnie z rozporządzeniem (UE) nr 1025/2012. Pojęcie „inteligentnej umowy" przewidziane w niniejszym rozporządzeniu jest technologicznie neutralne. Inteligentne umowy mogą być np. połączone z rejestrem elektronicznym. Zasadnicze wymagania powinny mieć zastosowanie wyłącznie do sprzedawców inteligentnych umów, jednak nie w przypadku gdy opracowują oni inteligentne umowy wewnątrz przedsiębiorstwa wyłącznie na użytek wewnętrzny. Zasadnicze wymaganie polegające na zapewnieniu, by wykonywanie inteligentnych umów mogło być zawieszane i by inteligentne umowy mogły być rozwiązywane, zakłada wzajemną zgodę stron umowy o dzielenie się danymi. Stosowanie inteligentnych umów do automatycznego wykonywania umów o dzielenie się danymi pozostaje bez wpływu lub powinno pozostawać bez wpływu na stosowanie do umów o dzielenie się danymi stosownych przepisów prawa cywilnego, prawa zobowiązań i prawa ochrony konsumentów.

(105) Aby wykazać przestrzeganie zasadniczych wymagań niniejszego rozporządzenia, sprzedawca inteligentnej umowy lub w razie jego braku osoba, której działalność handlowa, gospodarcza lub zawodowa obejmuje zapewnianie innym inteligentnych umów w kontekście wykonywania umowy o udostępnianiu danych, lub jej części, w kontekście niniejszego rozporządzenia, powinna dokonać oceny zgodności i wydać deklarację zgodności UE. Taka ocena zgodności powinna podlegać ogólnym zasadom określonym w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 765/2008[1] oraz w decyzji Parlamentu Europejskiego i Rady (WE) nr 768/2008[2].

(106) Poza spoczywającym na zawodowych twórcach inteligentnych umów obowiązkiem przestrzegania zasadniczych wymagań ważne jest także, aby zachęcać tych uczestników przestrzeni danych, którzy oferują dane lub usługi oparte na danych innym uczestnikom w europejskich przestrzeniach danych lub pomiędzy nimi, do wspierania interoperacyjności narzędzi służących dzieleniu się danymi, w tym inteligentnych umów.

---

1 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

2 Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz.U. L 218 z 13.8.2008, s. 82).

(107) Państwa członkowskie powinny wyznaczyć co najmniej jeden właściwy organ w celu zapewnienia skutecznego stosowania i egzekwowania niniejszego rozporządzenia. Jeżeli państwo członkowskie wyznacza więcej niż jeden właściwy organ, powinno również wyznaczyć spośród nich koordynatora danych. Właściwe organy powinny ze sobą współpracować. Podczas wykonywania swoich uprawnień do prowadzenia postępowań zgodnie z mającymi zastosowanie procedurami krajowymi właściwe organy powinny móc wyszukiwać i pozyskiwać informacje, w szczególności związane z działalnością podmiotu podlegającą ich kompetencjom oraz, w tym w kontekście wspólnych postępowań, z należytym poszanowaniem faktu, że środki nadzoru i egzekwowania dotyczące podmiotu podlegającego kompetencjom innego państwa członkowskiego powinny być przyjmowane przez właściwy organ tego państwa członkowskiego, w stosownym przypadku, zgodnie z procedurami dotyczącymi współpracy transgranicznej. Właściwe organy powinny terminowo pomagać sobie nawzajem, w szczególności gdy właściwy organ w państwie członkowskim posiada informacje istotne dla postępowania prowadzonego przez właściwe organy w innych państwach członkowskich lub gdy jest w stanie zgromadzić takie informacje, do których nie mają dostępu właściwe organy w państwie członkowskim, w którym podmiot ma siedzibę. Dane właściwych organów i koordynatorów danych powinny się znaleźć w rejestrze publicznym prowadzonym przez Komisję. Koordynator danych może być dodatkowym pośrednikiem ułatwiającym współpracę w sytuacjach transgranicznych, przykładowo gdy właściwy organ z danego państwa członkowskiego nie wie, do jakiego organu w państwie członkowskim koordynatora danych się zwrócić, np. gdy sprawa wiąże się z więcej niż jednym właściwym organem lub sektorem. Koordynator danych powinien działać m.in. jako pojedynczy punkt kontaktowy we wszystkich kwestiach związanych ze stosowaniem niniejszego rozporządzenia. Jeżeli nie wyznaczono koordynatora danych, zadania przypisane koordynatorowi danych na podstawie niniejszego rozporządzenia powinien wziąć na siebie właściwy organ. Organy odpowiedzialne za nadzór nad przestrzeganiem prawa ochrony danych oraz właściwe organy wyznaczone na podstawie prawa Unii lub prawa krajowego powinny być odpowiedzialne za stosowanie niniejszego rozporządzenia w obszarach swoich kompetencji. Aby zapobiec konfliktom interesów, właściwe organy odpowiedzialne za stosowanie i egzekwowanie niniejszego rozporządzenia w obszarze udostępniania danych na wniosek wynikający z wyjątkowej potrzeby nie powinny korzystać z prawa występowania z takim wnioskiem.

(108) Aby osoby fizyczne i prawne mogły egzekwować swoje prawa wynikające z niniejszego rozporządzenia, powinny być uprawnione do dochodzenia roszczeń w związku z naruszeniem ich praw wynikających z niniejszego rozporządzenia poprzez składanie skarg. Koordynator danych powinien na wniosek udzielać osobom fizycznym i prawnym wszelkich informacji niezbędnych do złożenia skargi do odpowiedniego właściwego organu. Organy te powinny być zobowiązane do współpracy, by skarga została właściwie i w odpowiednim czasie rozpatrzona i rozstrzygnięta. Aby wykorzystać mechanizm sieci współpracy w zakresie ochrony konsumenta i umożliwić występowanie z powództwem przedstawicielskim, niniejsze rozporządzenie zmienia załączniki do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2394[1] oraz do dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/1828[2].

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004 (Dz.U. L 345 z 27.12.2017, s. 1).

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/1828 z dnia 25 listopada 2020 r. w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów i uchylająca dyrektywę 2009/22/WE (Dz.U. L 409 z 4.12.2020, s. 1).

(109) Właściwe organy powinny zapewnić, aby naruszenia obowiązków ustanowionych w niniejszym rozporządzeniu podlegały karom. Karami takimi mogą być m.in. kary pieniężne, ostrzeżenia, nagany lub nakazy uzgodnienia praktyk biznesowych z obowiązkami nałożonymi niniejszym rozporządzeniem. Kary ustanowione przez państwa członkowskie powinny być skuteczne, proporcjonalne i odstraszające i powinny uwzględniać zalecenia Europejskiej Rady ds. Innowacji w zakresie Danych, a tym samym przyczyniać się do jak największej spójności w ustanawianiu i stosowaniu kar. W stosownym przypadku właściwe organy powinny posługiwać się środkami tymczasowymi, aby ograniczyć skutki domniemanego naruszenia, w czasie gdy trwa postępowanie w sprawie tego naruszenia. Powinny przy tym brać pod uwagę m.in. charakter, wagę, skalę i czas trwania naruszenia, mając na względzie określony interes publiczny, zakres i rodzaj prowadzonej działalności oraz możliwości ekonomiczne podmiotu naruszającego. Powinny one także uwzględniać, czy sprawca naruszenia systematycznie lub w sposób powtarzający się nie wypełnia swoich obowiązków wynikających z niniejszego rozporządzenia. Aby zapewnić poszanowanie zasady *ne bis in idem*, a w szczególności zapobiec sytuacji, w której to samo naruszenie niniejszego rozporządzenia skutkuje karą więcej niż jeden raz, każde państwo członkowskie, które zamierza wykonać swoje kompetencje wobec podmiotu naruszającego, który nie został ustanowiony i który nie wyznaczył przedstawiciela prawnego w Unii, powinno bez zbędnej zwłoki poinformować wszystkich koordynatorów danych oraz Komisję.

(110) Europejska Rada ds. Innowacji w zakresie Danych powinna doradzać i pomagać Komisji w koordynowaniu krajowych praktyk i polityk w sprawach objętych niniejszym rozporządzeniem oraz w realizacji jego celów związanych z normalizacją techniczną służącą zwiększeniu interoperacyjności. Powinna także odgrywać kluczową rolę w ułatwianiu kompleksowych dyskusji między właściwymi organami na temat stosowania i egzekwowania niniejszego rozporządzenia. Ta wymiana informacji ma służyć zwiększeniu skutecznego dostępu do wymiaru sprawiedliwości oraz egzekwowaniu przepisów i współpracy sądowej w całej Unii. Właściwe organy powinny korzystać m.in. z funkcji Europejskiej Rady ds. Innowacji w zakresie Danych jako platformy do oceny, koordynacji i przyjmowania zaleceń w sprawie ustalania kar za naruszanie niniejszego rozporządzenia. Powinna ona umożliwić właściwym organom, z pomocą Komisji, skoordynowanie optymalnego podejścia do określania i nakładania takich kar. Podejście to zapobiega rozdrobnieniu, a zarazem daje państwom członkowskim elastyczność i powinno skutkować skutecznymi zaleceniami wspierającymi spójne stosowanie niniejszego rozporządzenia. Europejska Rada ds. Innowacji w zakresie Danych powinna także pełnić rolę doradczą w procesach normalizacji i w przyjmowaniu wspólnych specyfikacji w formie aktów wykonawczych, w przyjmowaniu aktów delegowanych ustanawiających mechanizm monitorowania opłat z tytułu zmiany dostawcy nakładanych przez dostawców usług przetwarzania danych oraz doprecyzowujących zasadnicze wymagania na potrzeby interoperacyjności danych, w przyjmowaniu mechanizmów i usług dzielenia się danymi oraz wspólnych europejskich przestrzeni danych. Powinna także doradzać i pomagać Komisji w przyjmowaniu wytycznych ustanawiających specyfikacje w zakresie interoperacyjności na potrzeby funkcjonowania wspólnych europejskich przestrzeni danych.

(111) Aby pomóc przedsiębiorstwom w opracowywaniu i negocjowaniu umów, Komisja powinna opracować i zalecić niewiążące modelowe postanowienia umowne na potrzeby kontraktów w sprawie dzielenia się danymi między przedsiębiorcami, w razie potrzeby z uwzględnieniem warunków panujących w poszczególnych sektorach i obowiązujących praktyk w zakresie mechanizmów dobrowolnego dzielenia się danymi. Te modelowe postanowienia umowne powinny być przede wszystkim praktycznym narzędziem pomagającym zwłaszcza MŚP w zawieraniu umów. Jeżeli te modelowe postanowienia umowne będą stosowane powszechnie i w całości, powinny mieć również korzystny wpływ na kształt umów w sprawie dostępu do danych i ich wykorzystywania, a tym samym prowadzić w szerszym ujęciu do bardziej sprawiedliwych stosunków umownych przy dostępie do danych i dzieleniu się danymi.

(112) Aby wyeliminować ryzyko, że posiadacze danych w bazach danych pozyskanych lub wygenerowanych za pomocą elementów fizycznych, takich jak czujniki, produktu skomunikowanego i usługi powiązanej lub innych maszynowo wygenerowanych danych będą powoływać się na prawo *sui generis* określone w art. 7 dyrektywy 96/9/WE, a tym samym będą w szczególności ograniczać skuteczne wykonywanie przysługującego użytkownikom prawa dostępu do danych i ich wykorzystywania oraz prawo dzielenia się danymi z osobami trzecimi na podstawie niniejszego rozporządzenia, należy doprecyzować, że prawo *sui generis* nie ma zastosowania do takich baz danych. Nie wpływa to na możliwe stosowanie prawa *sui generis* określonego w art. 7 dyrektywy 96/9/WE względem baz danych zawierających dane niewchodzące w zakres niniejszego rozporządzenia, o ile spełnione są wymagania ochrony zgodnie z ust. 1 tego artykułu.

(113) W celu uwzględnienia aspektów technicznych usług przetwarzania danych, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w odniesieniu do uzupełnienia niniejszego rozporządzenia w celu wprowadzenia mechanizmu monitorowania opłat z tytułu zmiany dostawcy nakładanych na rynku przez dostawców usług przetwarzania danych i doprecyzowania zasadniczych wymagań w zakresie interoperacyjności wobec uczestników przestrzeni danych, którzy oferują innym uczestnikom dane lub usługi oparte na danych. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowane 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[1]. 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 przygotowywaniem aktów delegowanych.

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

(114) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu przyjęcia wspólnych specyfikacji służących zapewnieniu interoperacyjności danych, mechanizmów wymiany danych i usług, a także wspólnych europejskich przestrzeni danych, wspólnych specyfikacji interoperacyjności usług przetwarzania danych, oraz w odniesieniu do przyjęcia wspólnych specyfikacji dotyczących inteligentnych umów. Należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do publikowania odniesień do zharmonizowanych norm oraz wspólnych specyfikacji interoperacyjności usług przetwarzania danych w centralnym repozytorium norm Unii dotyczących interoperacyjności przetwarzania danych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[1].

(115) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla przepisów dotyczących specyficznych potrzeb poszczególnych sektorów lub obszarów służących interesowi publicznemu. Przepisy takie mogą obejmować dodatkowe wymagania dotyczące technicznych aspektów dostępu do danych, takich jak interfejsy dostępu do danych, lub sposobu zapewniania dostępu do danych, np. bezpośrednio z produktu lub poprzez usługi pośrednictwa danych. Przepisy takie mogą również obejmować ograniczenia praw posiadaczy danych do dostępu do danych użytkowników lub do ich wykorzystywania lub inne aspekty wykraczające poza dostęp do danych i ich wykorzystywanie, takie jak aspekty zarządzania lub wymagania bezpieczeństwa, w tym cyberbezpieczeństwa. Niniejsze rozporządzenie powinno również pozostawać bez uszczerbku dla bardziej szczególnych przepisów z zakresu rozwoju wspólnych europejskich przestrzeni danych lub dla prawa Unii i prawa krajowego przewidujących dostęp do danych na potrzeby badań naukowych i zezwalających na ich wykorzystywanie, z zastrzeżeniem wyjątków przewidzianych w niniejszym rozporządzeniu.

---

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

(116) Niniejsze rozporządzenie nie powinno wpływać 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.

(117) Aby umożliwić podmiotom wchodzącym w zakres stosowania niniejszego rozporządzenia dostosowanie się do nowych przepisów przewidzianych w nim i na dokonanie niezbędnych uzgodnień technicznych, przepisy te powinny zacząć obowiązywać od dnia... [20 miesięcy od dnia wejścia w życie niniejszego rozporządzenia].

(118) Zgodnie z art. 42 ust. 1 i 2 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, którzy wydali opinie w dniu 4 maja 2022 r.

(119) Ponieważ cele niniejszego rozporządzenia, a mianowicie zapewnienie sprawiedliwego podziału wartości z danych między podmiotami gospodarki opartej na danych oraz wspieranie sprawiedliwego dostępu do danych i ich wykorzystywania w celu przyczynienia się do ustanowienia prawdziwego rynku wewnętrznego danych, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na ich skalę i skutki, oraz transgraniczne wykorzystywanie danych, 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:

Rozdział I

Przepisy ogólne

Artykuł 1

Przedmiot i zakres stosowania

1. W niniejszym rozporządzeniu ustanawia się zharmonizowane przepisy między innymi dotyczące:

   a) udostępniania danych z produktu i z usługi powiązanej użytkownikowi produktu skomunikowanego lub usługi powiązanej;

   b) udostępniania danych przez posiadaczy danych odbiorcom danych;

   c) udostępniania danych przez posiadaczy danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu i organom Unii – w przypadku wystąpienia wyjątkowej potrzeby wykorzystania tych danych do celów wykonania określonego zadania realizowanego w interesie publicznym;

   d) ułatwiania zmiany dostawcy usług przetwarzania danych;

   e) wprowadzania zabezpieczeń przed niezgodnym z prawem dostępem osób trzecich do danych nieosobowych; oraz

   f) opracowania norm interoperacyjności wobec danych, które mają być udostępniane, przekazywane i wykorzystywane.

2. Niniejsze rozporządzenie dotyczy danych osobowych i nieosobowych, w tym następujących rodzajów danych i następujących kontekstów:

a) rozdział II ma zastosowanie do danych, z wyjątkiem treści, dotyczących działania, wykorzystywania i środowiska produktów skomunikowanych i usług powiązanych;

b) rozdział III ma zastosowanie do wszelkich danych sektora prywatnego podlegających ustawowym obowiązkom w zakresie dzielenia się danymi;

c) rozdział IV ma zastosowanie do wszelkich danych sektora prywatnego udostępnianych i wykorzystywanych na podstawie umów między przedsiębiorcami;

d) rozdział V ma zastosowanie do wszelkich danych sektora prywatnego ze szczególnym uwzględnieniem danych nieosobowych;

e) rozdział VI ma zastosowanie do wszelkich danych i usług przetwarzanych przez dostawców usług przetwarzania danych;

f) rozdział VII ma zastosowanie do wszelkich danych nieosobowych dostawców usług przetwarzania danych przechowywanych na terenie Unii.

3. Niniejsze rozporządzenie ma zastosowanie do:

a) producentów produktów skomunikowanych wprowadzanych do obrotu w Unii i dostawców usług powiązanych, niezależnie od miejsca siedziby tych producentów i dostawców;

b) znajdujących się w Unii użytkowników produktów skomunikowanych lub usług powiązanych, o których mowa w lit. a);

c) posiadaczy danych, którzy udostępniają dane odbiorcom danych w Unii, niezależnie od miejsca siedziby tych posiadaczy;

d) odbiorców danych w Unii, którym dane są udostępniane;

e) organów sektora publicznego, Komisji, Europejskiego Banku Centralnego oraz organów Unii, które w przypadku wyjątkowej potrzeby wykorzystania tych danych występują do posiadaczy danych z wnioskiem o udostępnienie danych do celów wykonania określonego zadania realizowanego w interesie publicznym, oraz posiadaczy danych, którzy dostarczają tych danych w odpowiedzi na taki wniosek;

f) dostawców usług przetwarzania danych świadczących takie usługi klientom w Unii, niezależnie od miejsca siedziby tych dostawców;

g) uczestników przestrzeni danych oraz sprzedawców aplikacji korzystających z inteligentnych umów, a także osób, których działalność handlowa, gospodarcza lub zawodowa obejmuje wdrażanie inteligentnych umów w ramach wykonywania umowy.

4. W przypadku gdy w niniejszym rozporządzeniu mowa jest o produktach skomunikowanych lub usługach powiązanych, takie odniesienia rozumie się jako obejmujące również wirtualnych asystentów, o ile wchodzą oni w interakcje z produktem skomunikowanym lub usługą powiązaną.

5. Niniejsze rozporządzenie pozostaje bez uszczerbku dla prawa Unii i prawa krajowego dotyczących ochrony danych osobowych, prywatności i poufności komunikacji oraz integralności urządzeń końcowych, które mają zastosowanie do danych osobowych przetwarzanych w związku z prawami i obowiązkami ustanowionymi w niniejszym rozporządzeniu, w szczególności dla rozporządzenia (UE) 2016/679 i rozporządzenia (UE) 2018/1725 oraz dyrektywy 2002/58/WE, w tym dla uprawnień i kompetencji organów nadzorczych oraz praw osób, których dane dotyczą. W przypadku gdy użytkownicy są osobami, których dane dotyczą, prawa ustanowione w rozdziale II niniejszego rozporządzenia są uzupełnieniem ich prawa dostępu i prawa do przenoszenia danych na mocy art. 15 i 20 rozporządzenia (UE) 2016/679. W razie kolizji pomiędzy niniejszym rozporządzeniem a prawem Unii dotyczącym ochrony danych osobowych lub prywatności lub prawem krajowym przyjętym zgodnie z takim prawem Unii pierwszeństwo ma stosowne prawo Unii lub prawo krajowe dotyczące ochrony danych osobowych lub prywatności.

6. Niniejsze rozporządzenie nie ma zastosowania do ani nie wyklucza dobrowolnych uzgodnień dotyczących wymiany danych między podmiotami prywatnymi i publicznymi, w szczególności dobrowolnych uzgodnień dotyczących dzielenia się danymi.

Niniejsze rozporządzenie nie wpływa na unijne i krajowe akty prawne przewidujące dzielenie się danymi, dostęp do nich i ich wykorzystywanie do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar, lub do celów celnych i podatkowych, w szczególności na rozporządzenia (UE) 2021/784, (UE) 2022/2065 i (UE) 2023/1543, dyrektywę (UE) 2023/1543, ani na współpracę międzynarodową w tej dziedzinie. Niniejsze rozporządzenie nie ma zastosowania do zbierania danych, dzielenia się nimi i ich wykorzystywania lub dostępu do danych na mocy rozporządzenia (UE) 2015/847 oraz dyrektywy (UE) 2015/849. Niniejsze rozporządzenie nie ma zastosowania do dziedzin niewchodzących w zakres prawa Unii i w żadnym wypadku nie wpływa na kompetencje państw członkowskich dotyczące bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu, któremu państwa członkowskie powierzyły wykonywanie zadań związanych z tymi kompetencjami, ani od ich uprawnień do ochrony innych zasadniczych funkcji państwa, w tym zapewniania integralności terytorialnej państwa oraz utrzymywania porządku publicznego. Niniejsze rozporządzenie nie wpływa na kompetencje państw członkowskich dotyczące administracji celnej i podatkowej lub zdrowia i bezpieczeństwa obywateli.

7. Niniejsze rozporządzenie uzupełnia podejście samoregulacyjne przewidziane w rozporządzeniu (UE) 2018/1807 poprzez wprowadzenie dodatkowych obowiązków o zasięgu ogólnym dotyczących zmiany dostawców w chmurze..

8. Niniejsze rozporządzenie pozostaje bez uszczerbku dla unijnych i krajowych aktów prawnych przewidujących ochronę praw własności intelektualnej, w szczególności dyrektywy 2001/29/WE, 2004/48/WE oraz (UE) 2019/790.

9. Niniejsze rozporządzenie pozostaje bez uszczerbku dla prawa unijnego i jest uzupełnieniem tego prawa służącego wspieraniu interesów konsumentów, zapewnianiu konsumentom wysokiego poziomu ochrony oraz ochronie ich zdrowia, bezpieczeństwa i interesów ekonomicznych, w szczególności dyrektywy 93/13/EWG, 2005/29/WE i 2011/83/UE.

10. Niniejsze rozporządzenie nie uniemożliwia zawierania umów o dobrowolnym, zgodnym z prawem dzieleniu się danymi, w tym umów zawieranych na zasadzie wzajemności, które są zgodne z wymogami określonymi w niniejszym rozporządzeniu.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

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

2) „metadane” oznaczają ustrukturyzowany opis treści danych lub sposobu wykorzystywania danych, który ułatwia wyszukiwanie lub wykorzystywanie tych danych;

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

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

5) „produkt skomunikowany” oznacza rzecz, która pozyskuje, generuje lub zbiera dostępne dane dotyczące jej wykorzystywania lub jej otoczenia i która jest w stanie komunikować dane z produktu za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu i której podstawową funkcją nie jest przechowywanie, przetwarzanie ani przesyłanie danych w imieniu strony innej niż użytkownik;

6) „usługa powiązana” oznacza usługę cyfrową, w tym oprogramowanie, ale z wyłączeniem usług łączności elektronicznej, która podczas zakupu, najmu, dzierżawy lub leasingu jest skomunikowana z produktem w taki sposób, że jej brak uniemożliwiłby produktowi skomunikowanemu wykonywanie co najmniej jednej z jego funkcji, lub która zostaje skomunikowana z produktem przez producenta lub osobę trzecią później, aby dodać, uaktualnić lub zmodyfikować funkcje produktu skomunikowanego;

7) „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych lub zestawach danych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

8) „usługa przetwarzania danych” oznacza świadczoną na rzecz klienta usługę cyfrową umożliwiającą wszechobecny sieciowy dostęp na żądanie do wspólnego zbioru konfigurowalnych, skalowalnych i elastycznych zasobów obliczeniowych o charakterze scentralizowanym, rozproszonym lub wysoce rozproszonym, które mogą być szybko przydzielone i uwolnione przy minimalnym wysiłku pod względem zarządzania lub interakcji z dostawcą usług;

9) „usługa tego samego typu” oznacza zestaw usług przetwarzania danych, które mają ten sam główny cel, opierają się na tym samym modelu usługi przetwarzania danych i mają te same najważniejsze funkcje;

10) „usługa pośrednictwa danych” oznacza usługę pośrednictwa danych zdefiniowaną w art. 2 pkt 11 rozporządzenia (UE) 2022/868;

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

12) „użytkownik” oznacza osobę fizyczną lub prawną, która jest właścicielem produktu skomunikowanego lub której na podstawie umowy przekazane zostały tymczasowe prawa do korzystania z tego produktu skomunikowanego, lub która korzysta z usług powiązanych;

13) „posiadacz danych” oznacza osobę fizyczną lub prawną, która ma prawo lub obowiązek – zgodnie z niniejszym rozporządzeniem, mającym zastosowanie prawem Unii lub prawem krajowym przyjętym zgodnie z prawem Unii – wykorzystywać i udostępniać dane, w tym o ile zostało to przewidziane umową, dane z produktu lub dane z usługi powiązanej pobrane lub wygenerowane przez nią podczas świadczenia powiązanej usługi;

14) „odbiorca danych” oznacza osobę fizyczną lub prawną działającą w celach związanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, inną niż użytkownik produktu skomunikowanego lub usługi powiązanej, której to osobie posiadacz danych udostępnia dane, w tym osobę trzecią na wniosek użytkownika skierowany do posiadacza danych lub zgodnie z obowiązkiem prawnym wynikającym z prawa Unii lub prawem krajowym przyjętym zgodnie z prawem Unii;

15) „dane z produktu” oznaczają dane wygenerowane w wyniku korzystania z produktu skomunikowanego, które producent zaprojektował tak, by użytkownik, posiadacz danych lub osoba trzecia, w tym w stosownym przypadku producent, mogli je pobierać za pomocą usługi łączności elektronicznej, łącza fizycznego lub dostępu na urządzeniu;

16) „dane z usługi powiązanej” oznaczają dane stanowiące cyfrowe odwzorowanie czynności lub zdarzeń z udziałem użytkownika związanych z produktem skomunikowanym, utrwalane przez użytkownika celowo lub generowane jako produkt uboczny jego czynności, podczas świadczenia usługi powiązanej przez dostawcę;

17) „dane łatwo dostępne” oznaczają dane z produktu i dane z usługi powiązanej, które posiadacz danych zgodnie z prawem pozyskuje lub może zgodnie z prawem pozyskać z produktu skomunikowanego lub z usługi powiązanej bez nieproporcjonalnie dużego wysiłku wykraczającego poza prostą czynność;

18) „tajemnica przedsiębiorstwa” oznacza tajemnicę przedsiębiorstwa zdefiniowaną w art. 2 pkt 1 dyrektywy (UE) 2016/943;

19) „posiadacz tajemnicy przedsiębiorstwa” oznacza posiadacza tajemnicy przedsiębiorstwa zdefiniowanego w art. 2 pkt 2 dyrektywy (UE) 2016/943;

20) „profilowanie” oznacza profilowanie zdefiniowane w art. 4 pkt 4 rozporządzenia (UE) 2016/679;

21) „udostępnienie na rynku” oznacza każde dostarczenie produktu skomunikowanego na rynek Unii w celu jego dystrybucji, konsumpcji lub wykorzystywania w ramach działalności handlowej, odpłatnie lub nieodpłatnie;

22) „wprowadzenie do obrotu” oznacza udostępnienie produktu skomunikowanego na rynku Unii po raz pierwszy;

23) „konsument” oznacza osobę fizyczną działającą w celach, które nie mieszczą się w ramach jej działalności handlowej, gospodarczej, rzemieślniczej lub zawodowej;

24) „przedsiębiorstwo” oznacza osobę fizyczną lub prawną, która w związku z umowami i praktykami objętymi niniejszym rozporządzeniem działa w celach związanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub zawodową;

25) „małe przedsiębiorstwo” oznacza małe przedsiębiorstwo zdefiniowane w art. 2 ust. 2 zalecenia 2003/361/WE;

26) „mikroprzedsiębiorstwo” oznacza mikroprzedsiębiorstwo zdefiniowane w art. 2 ust. 3 załącznika do zalecenia 2003/361/WE;

27) „organy Unii” oznaczają organy i jednostki organizacyjne Unii ustanowione na mocy aktów przyjętych na podstawie Traktatu o Unii Europejskiej, TFUE lub Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej lub zgodnie z nimi;

28) „organ sektora publicznego” oznacza organy krajowe, regionalne lub lokalne państw członkowskich oraz podmioty prawa publicznego państw członkowskich lub związki złożone z co najmniej jednego takiego organu lub z co najmniej jednego takiego podmiotu;

29) „niebezpieczeństwo publiczne” oznacza ograniczoną w czasie sytuację wyjątkową, taką jak stan zagrożenia zdrowia publicznego, sytuacja nadzwyczajna w wyniku klęski żywiołowej, poważna katastrofa spowodowana przez człowieka, w tym poważny cyberincydent, która to sytuacja negatywnie wpływa na ludność Unii, państwa członkowskiego lub ich części i wiąże się z ryzykiem wystąpienia poważnych i trwałych następstw dla warunków życia lub stabilności gospodarczej, stabilności finansowej lub z ryzykiem znacznego i natychmiastowego obniżenia wartości aktywów gospodarczych w Unii lub w odpowiednim państwie członkowskim i którą stwierdza się lub oficjalnie ogłasza zgodnie z odpowiednimi procedurami przewidzianymi w prawie Unii lub prawie krajowym;

30) „klient” oznacza osobę fizyczną lub prawną, która nawiązała stosunek umowny z dostawcą usług przetwarzania danych w celu skorzystania z co najmniej jednej usługi przetwarzania danych;

31) „wirtualni asystenci” oznaczają oprogramowanie, które może przetwarzać żądania, zadania lub pytania, w tym na podstawie dźwięku, pisma, gestów lub ruchów, i które na podstawie tych żądań, zadań lub pytań zapewnia dostęp do innych usług lub kontroluje funkcje produktów skomunikowanych;

32) „aktywa cyfrowe” oznaczają elementy w formacie cyfrowym, w tym aplikacje, z których klient ma prawo korzystać, niezależnie od stosunku umownego obejmującego usługę przetwarzania danych, której dostawcę zamierza zmienić;

33) „lokalna infrastruktura ICT” oznacza infrastrukturę ICT i zasoby obliczeniowe będące własnością klienta, przedmiotem najmu, dzierżawy lub leasingu przez niego, znajdujące się w jego własnym centrum danych i obsługiwane przez tego klienta lub osobę trzecią;

34) „zmiana dostawcy” oznacza proces, w którym uczestniczą wyjściowy dostawca usług przetwarzania danych, klient korzystający z usługi przetwarzania danych oraz, w odpowiednich przypadkach, docelowy dostawca usług przetwarzania danych i w ramach którego klient korzystający z usługi przetwarzania danych przechodzi od korzystania z jednej usługi przetwarzania danych do korzystania z innej usługi tego samego typu lub z innej usługi oferowanych przez innego dostawcę usług przetwarzania danych, lub z lokalnej infrastruktury ICT, w tym poprzez ekstrakcję, transformację i załadowanie danych;

35) „opłaty z tytułu wychodzącego ruchu danych” oznaczają opłaty za przekazanie danych pobierane od klientów za ekstrakcję ich danych przez sieć z infrastruktury ICT dostawcy usług przetwarzania danych do systemów innego dostawcy lub do infrastruktury lokalnej ICT;

36) „opłaty z tytułu zmiany dostawcy” oznaczają opłaty – inne niż standardowe opłaty za usługę lub kary za wcześniejsze rozwiązanie umowy – nakładane przez dostawcę usług przetwarzania danych na klienta za działania wymagane zgodnie z niniejszym rozporządzeniem w celu zmiany na system innego dostawcy lub lokalną infrastrukturę ICT, w tym opłaty z tytułu wychodzącego ruchu danych;

37) „równoważność funkcjonalna” oznacza przywrócenie – na podstawie danych eksportowalnych i aktywów cyfrowych klienta – minimalnego poziomu funkcjonalności w środowisku nowej usługi przetwarzania danych tego samego typu po procesie zmiany dostawcy, przy czym usługa docelowa przetwarzania danych daje zasadniczo porównywalny rezultat w odpowiedzi na te same dane wejściowe dla jednakowych funkcji dostarczanych klientowi na podstawie umowy;

38) „dane eksportowalne” do celów art. 23 do 31 i art. 35 oznaczają dane wejściowe i wyjściowe, w tym metadane, bezpośrednio lub pośrednio wygenerowane bądź współwygenerowane w wyniku korzystania przez klienta z usługi przetwarzania danych zapewnianej przez dostawców usług przetwarzania danych lub osoby trzecie, z wyłączeniem wszelkich aktywów lub danych, które są objęte prawami własności intelektualnej lub są tajemnicami przedsiębiorstwa;

39) „inteligentna umowa” oznacza program komputerowy stosowany do automatycznego wykonywania umowy lub jej części, używający sekwencji elektronicznych rekordów danych i zapewniający ich integralność i dokładność ich chronologicznego uporządkowania;

40) „interoperacyjność” oznacza zdolność co najmniej dwóch przestrzeni danych lub sieci komunikacyjnych, systemów, produktów skomunikowanych, aplikacji, usług przetwarzania danych lub komponentów do wymiany i wykorzystywania danych w celu wykonywania swoich funkcji;

41) „otwarte specyfikacje w zakresie interoperacyjności” oznaczają specyfikacje techniczne w dziedzinie ICT, które są ukierunkowane na osiągnięcie interoperacyjności między usługami przetwarzania danych;

42) „wspólne specyfikacje” oznaczają dokument inny niż norma, zawierający rozwiązania techniczne zapewniające środki umożliwiające przestrzeganie niektórych wymagań i obowiązków ustanowionych na podstawie niniejszego rozporządzenia;

43) „norma zharmonizowana” oznacza normę zharmonizowaną zdefiniowaną w art. 2 pkt 1 lit. c) rozporządzenia (UE) nr 1025/2012;

Rozdział II
Dzielenie się danymi przez przedsiębiorców z konsumentami i z innymi przedsiębiorcami

Artykuł 3

Obowiązek udostępniania danych z produktu i z usługi powiązanej użytkownikowi

1. Produkty skomunikowane są projektowane i produkowane, a usługi powiązane projektowane i świadczone w taki sposób, aby dane z produktu i z usługi powiązanej, w tym stosowne metadane niezbędne do interpretacji i wykorzystania danych, były domyślnie łatwo, bezpiecznie, bezpłatnie, w całościowym, ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie oraz, w stosownym przypadku i jeśli jest to technicznie możliwe, bezpośrednio dostępne dla użytkownika.

2. Zanim zawarta zostanie umowa sprzedaży, najmu, dzierżawy lub leasingu produktu skomunikowanego, sprzedawca, wynajmujący, wydzierżawiający lub leasingodawca, którym może być producent, przedstawiają użytkownikowi w jasny i zrozumiały sposób co najmniej następujące informacje:

   a) rodzaj, format i szacunkową ilość danych z produktu, które produkt skomunikowany jest w stanie wygenerować;

   b) czy produkt skomunikowany jest w stanie generować dane w sposób ciągły i w czasie rzeczywistym;

   c) czy produkt skomunikowany jest w stanie przechowywać dane na urządzeniu lub na zdalnym serwerze, w tym w stosownym przypadku zamierzony okres zatrzymywania danych;

d) w jaki sposób użytkownik może uzyskać dostęp do tych danych, pobrać je lub w stosownym przypadku usunąć, w tym środki techniczne stosowane w tym celu, a także warunki ich wykorzystywania i jakość usługi.

3. Zanim zawarta zostanie umowa o świadczenie usługi powiązanej, dostawca takiej usługi zapewnia użytkownikowi w jasny i zrozumiały sposób co najmniej następujące informacje:

a) charakter, szacunkową ilość i częstotliwość zbierania danych z produktu, które ma pozyskiwać przyszły posiadacz danych, oraz w stosownym przypadku uzgodnienia dotyczące dostępu użytkownika do takich danych lub ich pobierania, w tym uzgodnienia dotyczące przechowywania i okresu zatrzymywania danych przyszłego posiadacza danych;

b) charakter i szacunkową ilość danych z usługi powiązanej, które będą generowane, oraz uzgodnienia dotyczące dostępu użytkownika do takich danych lub ich pobierania, w tym uzgodnienia dotyczące przechowywania i okresu zatrzymywania danych przyszłego posiadacza danych;

c) czy przyszły posiadacz danych planuje sam wykorzystywać dane łatwo dostępne i cele, w których dane te będą wykorzystywane, oraz czy zamierza zezwolić co najmniej jednej osobie trzeciej na wykorzystywanie danych do celów uzgodnionych z użytkownikiem;

d) tożsamość przyszłego posiadacza danych, taką jak jego nazwę handlową i adres geograficzny, pod którym ma siedzibę, oraz w stosownym przypadku tożsamość innych osób przetwarzających dane;

e) środki komunikacji umożliwiające szybki kontakt z przyszłym posiadaczem danych i sprawną komunikację z tym posiadaczem danych;

f) w jaki sposób użytkownik może wystąpić z wnioskiem o dzielenie się danymi z osobą trzecią i w stosownym przypadku zakończyć dzielenie się danymi;

g) prawo użytkownika do wniesienia skargi dotyczącej naruszenia przepisów niniejszego rozdziału do właściwego organu wyznaczonego zgodnie z art. 37;

h) czy przyszły posiadacz danych jest posiadaczem tajemnic przedsiębiorstwa zawartych w danych, do których łatwo będzie można uzyskać dostęp z produktu skomunikowanego lub które będą generowane w trakcie świadczenia usługi powiązanej, a jeśli przyszły posiadacz danych nie jest posiadaczem tajemnic przedsiębiorstwa, jaka jest tożsamość posiadacza tajemnic przedsiębiorstwa;

i) okres obowiązywania umowy między użytkownikiem a przyszłym posiadaczem danych oraz uzgodnienia dotyczące rozwiązania takiej umowy.

Artykuł 4

Prawa i obowiązki użytkowników i posiadaczy danych w odniesieniu do dostępu do danych z produktu i z usługi powiązanej, ich wykorzystywania i udostępniania

1. W przypadku gdy użytkownik nie może uzyskać bezpośredniego dostępu do danych z produktu skomunikowanego lub z usługi powiązanej, posiadacze danych bez zbędnej zwłoki, w sposób łatwy i bezpieczny, nieodpłatnie udostępniają użytkownikowi dane łatwo dostępne, wraz z odpowiednimi metadanymi niezbędnymi do interpretacji i wykorzystania tych danych, cechujące się taką samą jakością, jaka jest dostępna dla posiadacza danych, w całościowym, ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego formacie oraz w stosownym przypadku i jeżeli jest to technicznie wykonalne – w sposób ciągły i w czasie rzeczywistym. Odbywa się to na podstawie zwykłego wniosku złożonego drogą elektroniczną, jeżeli jest to technicznie możliwe.

2. Użytkownicy i posiadacze danych mogą umownie ograniczyć lub zakazać dostępu do danych, ich wykorzystywania lub dalszego dzielenia się nimi, jeżeli takie przetwarzanie mogłoby zagrozić wymaganiom bezpieczeństwa produktu skomunikowanego określonym w prawie Unii lub prawie krajowym i mieć poważny negatywny wpływ na zdrowie, bezpieczeństwo lub ochronę osób fizycznych. Organy sektorowe mogą zapewnić użytkownikom i posiadaczom danych fachową wiedzę techniczną w tym kontekście. W przypadku gdy posiadacz danych odmawia dzielenia się danymi na podstawie niniejszego artykułu, powiadamia on właściwy organ wyznaczony zgodnie z art. 37.

3. Bez uszczerbku dla przysługującego użytkownikowi w dowolnym momencie prawa do dochodzenia roszczeń przed sądem lub trybunałem państwa członkowskiego, użytkownik może w związku ze sporem z posiadaczem danych w sprawie ograniczeń umownych lub zakazów, o których mowa w ust. 2:

   a) wnieść skargę do właściwego organu zgodnie z art. 37 ust. 5 lit. b); lub

   b) uzgodnić z posiadaczem danych wniesienie sprawy do organu rozstrzygania sporów zgodnie z art. 10 ust. 1.

4. Posiadacze danych nie utrudniają bezzasadnie użytkownikom dokonywania wyborów ani wykonywania praw na podstawie niniejszego artykułu, w tym poprzez oferowanie użytkownikom wyboru w sposób nieneutralny lub poprzez podważanie lub ograniczanie autonomii, zdolności decyzyjnych lub wyborów użytkownika za pomocą struktury, projektu, funkcji lub sposobu działania interfejsu cyfrowego użytkownika bądź jego części.

5. W celu kontroli, czy osoba fizyczna lub prawna kwalifikuje się jako użytkownik na potrzeby ust. 1, posiadacz danych nie wymaga od użytkownika dostarczenia żadnych informacji poza tymi, które są niezbędne. Posiadacze danych nie zachowują żadnych informacji, w szczególności danych z rejestru zdarzeń, na temat dostępu użytkownika do żądanych danych poza informacjami, które są niezbędne do należytego wykonania wniosku użytkownika o dostęp oraz do zapewnienia bezpieczeństwa i utrzymania infrastruktury danych.

6. Chroni się tajemnice przedsiębiorstwa i ujawnia się je wyłącznie wtedy, gdy posiadacz danych i użytkownik przed ujawnieniem zastosują wszelkie środki niezbędne do ochrony ich poufności, w szczególności w odniesieniu do osób trzecich. Posiadacz danych lub, jeżeli nie jest to ta sama osoba, posiadacz tajemnicy przedsiębiorstwa identyfikują dane chronione, w tym stosowne metadane, jako tajemnice przedsiębiorstwa i uzgadniają z użytkownikiem proporcjonalne środki techniczne i organizacyjne niezbędne do ochrony poufności danych podlegających dzieleniu się, w szczególności w odniesieniu do osób trzecich, takie jak modelowe postanowienia umowne, umowy o poufności, protokoły ścisłego dostępu, normy techniczne oraz stosowanie kodeksów postępowania.

7. W przypadku gdy nie uzgodniono niezbędnych środków technicznych, o których mowa w ust. 6, lub gdy użytkownik nie wdraża środków uzgodnionych zgodnie z ust. 6 lub zagraża poufności tajemnic przedsiębiorstwa, posiadacz danych może wstrzymać lub w stosownym przypadku zawiesić dzielenie się danymi zidentyfikowanymi jako tajemnice przedsiębiorstwa. Posiadacz danych należycie uzasadnia decyzję i bez zbędnej zwłoki przekazuje ją na piśmie użytkownikowi. W takich przypadkach posiadacz danych powiadamia właściwy organ wyznaczony zgodnie z art. 37, że wstrzymał lub zawiesił dzielenie się danymi, i wskazuje, których środków nie wdrożono lub nie zastosowano, lub w stosownym przypadku poufność których tajemnic przedsiębiorstwa zagrożono.

8. W wyjątkowych okolicznościach, w przypadku gdy posiadacz danych będący posiadaczem tajemnicy przedsiębiorstwa może wykazać, że mimo środków technicznych i organizacyjnych zastosowanych przez użytkownika zgodnie z ust. 6 niniejszego artykułu ujawnienie tajemnic handlowych z dużym prawdopodobieństwem poskutkuje poważną szkodą ekonomiczną, posiadacz danych może w tym konkretnym przypadku odrzucić wniosek o dostęp do tych konkretnych danych. Wykazane informacje zostają należycie uzasadnione na podstawie obiektywnych elementów, w szczególności egzekwowalności tajemnic przedsiębiorstwa w krajach trzecich, charakteru i poziomu poufności żądanych danych oraz niepowtarzalności i nowatorskości produktu skomunikowanego, i przedstawione na piśmie bez zbędnej zwłoki. W przypadku gdy posiadacz danych odmawia dzielenia się danymi na podstawie niniejszego ustępu, powiadamia on właściwy organ wyznaczony zgodnie z art. 37.

9. Bez uszczerbku dla przysługującego użytkownikowi w dowolnym momencie prawa do dochodzenia roszczeń przed sądem lub trybunałem państwa członkowskiego, użytkownik chcący zaskarżyć decyzję posiadacza danych o odmowie, wstrzymaniu lub zawieszeniu dzielenia się danymi zgodnie z ust. 7 i 8 może:

   a) wnieść skargę zgodnie z art. 37 ust. 5 lit. b) do właściwego organu, który bez zbędnej zwłoki podejmuje decyzję, czy i na jakich warunkach dzielenie się danymi powinno się rozpocząć lub zostać wznowione; lub

   b) uzgodnić z posiadaczem danych wniesienie sprawy do organu rozstrzygania sporów zgodnie z art. 10 ust. 1.

10. Użytkownik nie wykorzystuje danych pozyskanych na podstawie wniosku, o którym mowa w ust. 1, do opracowania produktu skomunikowanego konkurującego z produktem skomunikowanym, z którego pochodzą dane, ani nie dzieli się w tym celu danymi z osobą trzecią i nie wykorzystuje takich danych do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji producenta lub w stosownym przypadku posiadacza danych.

11. Użytkownik nie stosuje środków przymusu ani nie nadużywa luk w infrastrukturze technicznej posiadacza danych, która ma chronić dane, w celu uzyskania dostępu do danych.

12. W przypadku gdy użytkownik nie jest osobą, której dotyczą dane osobowe objęte wnioskiem, wszelkie dane osobowe wygenerowane w wyniku korzystania z produktu skomunikowanego lub usługi powiązanej są udostępniane użytkownikowi przez posiadacza danych wyłącznie wtedy, gdy istnieje ważna podstawa prawna przetwarzania zgodnie z art. 6 rozporządzenia (UE) 2016/679 oraz w stosownym przypadku spełnione są warunki określone w art. 9 tego rozporządzenia i w art. 5 ust. 3 dyrektywy (UE) 2002/58.

13. Posiadacz danych wykorzystuje dane łatwo dostępne będące danymi nieosobowymi wyłącznie na podstawie umowy z użytkownikiem. Posiadacz danych nie wykorzystuje takich danych do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji użytkownika lub korzystaniu przez użytkownika, które to informacje mogłyby w inny sposób osłabić pozycję handlową użytkownika na rynkach jego działalności.

14. Posiadacze danych nie udostępniają danych nieosobowych z produktu osobom trzecim w celach handlowych lub niehandlowych innych niż realizacja umowy z użytkownikiem. W stosownych przypadkach posiadacze danych umownie zobowiązują osoby trzecie, aby nie dzieliły się dalej otrzymanymi od nich danymi.

Artykuł 5

Prawo użytkownika do dzielenia się danymi z osobami trzecimi

1. Na wniosek użytkownika lub strony działającej w jego imieniu posiadacz danych bez zbędnej zwłoki w sposób łatwy i bezpieczny oraz nieodpłatnie dla użytkownika udostępnia osobie trzeciej dane łatwo dostępne wraz z odpowiednimi metadanymi niezbędnymi do interpretacji i wykorzystania tych danych cechujące się taką samą jakością, jaka jest dostępna dla posiadacza danych, w całościowym, ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego formacie oraz w stosownym przypadku i jeżeli jest to technicznie możliwe – w sposób ciągły i w czasie rzeczywistym. Danych są udostępniane przez posiadacza danych osobie trzeciej zgodnie z art. 8 i 9.

2. Ust. 1 nie ma zastosowania do danych łatwo dostępnych w kontekście testowania nowych produktów skomunikowanych, substancji lub procesów, które nie zostały jeszcze wprowadzone do obrotu, chyba że ich wykorzystanie przez osobę trzecią jest dozwolone na podstawie umowy.

3. Przedsiębiorstwo wskazane jako strażnik dostępu na mocy art. 3 rozporządzenia (UE) 2022/1925 nie kwalifikuje się jako osoba trzecia na mocy niniejszego artykułu, a zatem:

   a) w żaden sposób nie nakłania ani komercyjnie nie zachęca użytkownika, w tym przez zapewnienie rekompensaty pieniężnej lub jakiejkolwiek innej, do udostępnienia danych, które użytkownik pozyskał na podstawie wniosku złożonego zgodnie z art. 4 ust. 1, na potrzeby jednej ze swoich usług;

   b) nie nakłania ani komercyjnie nie zachęca użytkownika do zwrócenia się do posiadacza danych z wnioskiem o udostępnienie danych na potrzeby jednej ze swoich usług zgodnie z ust. 1 niniejszego artykułu;

   c) nie otrzymuje danych od użytkownika, które użytkownik pozyskał na podstawie wniosku złożonego zgodnie z art. 4 ust. 1.

4. W celu kontroli, czy osoba fizyczna lub prawna kwalifikuje się jako użytkownik lub osoba trzecia w świetle ust. 1, użytkownik ani osoba trzecia nie muszą dostarczać żadnych informacji poza tymi, które są niezbędne. Posiadacze danych nie zachowują żadnych informacji na temat dostępu osoby trzeciej do żądanych danych poza informacjami, które są niezbędne do należytego wykonania wniosku osoby trzeciej o dostęp oraz do zapewnienia bezpieczeństwa i utrzymania infrastruktury danych.

5. Osoba trzecia nie stosuje środków przymusu ani nie nadużywa luk w infrastrukturze technicznej posiadacza danych, która ma chronić dane, w celu uzyskania dostępu do danych.

6. Posiadacz danych nie wykorzystuje danych łatwo dostępnych do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji osoby trzeciej lub korzystaniu przez osobę trzecią w inny sposób, które to informacje mogłyby osłabić pozycję handlową osoby trzeciej na rynkach jej działalności, chyba że osoba trzecia pozwoliła na takie wykorzystanie i ma techniczną możliwość łatwego wycofania tego pozwolenia w dowolnym momencie.

7. W przypadku gdy użytkownik nie jest osobą, której dotyczą dane osobowe objęte wnioskiem, wszelkie dane osobowe wygenerowane w wyniku korzystania z produktu skomunikowanego lub usługi powiązanej są udostępniane osobie trzeciej przez posiadacza danych, wyłącznie wtedy, gdy istnieje ważna podstawa prawna przetwarzania zgodnie z art. 6 rozporządzenia (UE) 2016/679, oraz gdy w stosownym przypadku spełnione są warunki określone w art. 9 tego rozporządzenia (UE) i w art. 5 ust. 3 dyrektywy 2022/58.

8. Wszelkie przypadki niedokonania przez posiadacza danych i osobę trzecią uzgodnień dotyczących przesyłania danych nie utrudniają, nie uniemożliwiają ani nie zakłócają wykonywania praw przysługujących osobie, której dane dotyczą, na podstawie rozporządzenia (UE) 2016/679, a w szczególności prawa do przenoszenia danych na podstawie w art. 20 tego rozporządzenia.

9. Chroni się tajemnice przedsiębiorstwa i ujawnia się je osobom trzecim wyłącznie w zakresie, w jakim jest to ściśle niezbędne do realizacji celu uzgodnionego przez użytkownika i osobę trzecią. Posiadacz danych lub, jeżeli nie jest to ta sama osoba, posiadacz tajemnicy przedsiębiorstwa identyfikują dane chronione jako tajemnice przedsiębiorstwa, w tym stosowne metadane, i uzgadniają z użytkownikiem wszelkie proporcjonalne środki techniczne i organizacyjne niezbędne do ochrony poufności danych będących przedmiotem dzielenia się, takie jak modelowe postanowienia umowne, umowy o poufności, protokoły ścisłego dostępu, normy techniczne oraz stosowanie kodeksów postępowania.

10. W przypadku gdy nie uzgodniono niezbędnych środków, o których mowa w ust. 9, lub gdy osoba trzecia nie wdraża środków uzgodnionych zgodnie z ust. 9 lub zagraża poufności tajemnic przedsiębiorstwa, posiadacz danych może wstrzymać lub w stosownym przypadku zawiesić dzielenie się danymi zidentyfikowanymi jako tajemnice przedsiębiorstwa. Posiadacz danych należycie uzasadnia decyzję i bez zbędnej zwłoki przekazuje ją na piśmie osobie trzeciej. W takich przypadkach posiadacz danych powiadamia właściwy organ wyznaczony zgodnie z art. 37, że wstrzymał lub zawiesił dzielenie się danymi, i wskazuje, których środków nie uzgodniono lub nie wdrożono lub w stosownym przypadku poufność których tajemnic przedsiębiorstwa zagrożono.

11. W wyjątkowych okolicznościach, kiedy posiadacz danych będący posiadaczem tajemnicy przedsiębiorstwa może wykazać, że mimo środków technicznych i organizacyjnych zastosowanych przez osobę trzecią zgodnie z art. 9 niniejszego artykułu, ujawnienie tajemnic handlowych z dużym prawdopodobieństwem poskutkuje poważną szkodą ekonomiczną, posiadacz danych może w tym konkretnym przypadku odrzucić wniosek o dostęp do tych konkretnych danych. Wykazane informacje zostają należycie uzasadnione na podstawie obiektywnych elementów, w szczególności egzekwowalności tajemnic przedsiębiorstwa w krajach trzecich, charakteru i poziomu poufności żądanych danych oraz niepowtarzalności i nowatorskości produktu, i przedstawione na piśmie bez zbędnej zwłoki. W przypadku gdy posiadacz danych odmawia dzielenia się danymi na podstawie niniejszego ustępu, powiadamia on właściwy organ wyznaczony zgodnie z art. 37.

12. Bez uszczerbku dla prawa do dochodzenia roszczeń w dowolnym momencie przed sądem lub trybunałem państwa członkowskiego, osoba trzecia chcąca zaskarżyć decyzję posiadacza danych o odmowie, wstrzymaniu lub zawieszeniu dzielenia się danymi zgodnie z ust. 10 i 11 może:

    a) wnieść skargę do właściwego organu zgodnie z art. 37 ust. 5 lit. b), który bez zbędnej zwłoki podejmuje decyzję, czy i na jakich warunkach dzielenie się danymi powinno się rozpocząć lub zostać wznowione; lub

    b) uzgodnić z posiadaczem danych wniesienie sprawy do organu rozstrzygania sporów zgodnie z art. 10 ust. 1.

13. Prawo, o którym mowa w ust. 1, nie wpływa niekorzystnie na prawa osób, których dane dotyczą, zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym dotyczącym ochrony danych osobowych lub prywatności.

Artykuł 6

Obowiązki osób trzecich otrzymujących dane na wniosek użytkownika

1. Osoba trzecia przetwarza dane udostępnione jej na podstawie art. 5 wyłącznie do celów i na warunkach uzgodnionych z użytkownikiem i – jeżeli spełnione są wszystkie warunki i zasady przewidziane w mającym zastosowanie prawie Unii lub prawie krajowym dotyczącym ochrony danych osobowych lub prywatności w tym prawach osoby, której dane dotyczą, w odniesieniu do danych osobowych. Osoba trzecia usuwa dane, gdy nie są one już niezbędne do uzgodnionego celu, chyba że uzgodniono inaczej z użytkownikiem w odniesieniu do danych nieosobowych.

2. Osoba trzecia:

   a) nie utrudnia bezzasadnie użytkownikom dokonywania wyborów i wykonywania praw na podstawie art. 5 i niniejszego artykułu, w tym poprzez oferowanie użytkownikom wyboru w sposób nieneutralny lub zmuszanie, wprowadzanie w błąd użytkownika lub manipulowanie nim, bądź podważanie lub ograniczanie autonomii, zdolności decyzyjnych lub wyborów użytkowników, w tym za pomocą cyfrowego interfejsu użytkownika lub za pomocą jego części;

   b) niezależnie od art. 22 ust. 2 lit. a) i c) rozporządzenia (UE) 2016/679 nie wykorzystuje otrzymanych danych do profilowania, chyba że jest to niezbędne do świadczenia usługi żądanej przez użytkownika;

c) nie udostępnia otrzymanych danych innej osobie trzeciej, chyba że udostępnia je na podstawie umowy z użytkownikiem, i pod warunkiem że ta inna osoba trzecia zastosuje wszystkie niezbędne środki uzgodnione między posiadaczem danych a osobą trzecią w celu ochrony poufności tajemnic przedsiębiorstwa;

d) nie udostępnia otrzymanych danych przedsiębiorstwu wskazanemu jako strażnik dostępu na podstawie art. 3 rozporządzenia (UE) 2022/1925;

e) nie wykorzystuje otrzymanych danych do opracowania produktu konkurującego z produktem skomunikowanym, z którego pochodzą dane, ani nie dzieli się nimi w tym celu z inną osobą trzecią; osoby trzecie nie wykorzystują też udostępnionych im danych nieosobowych z produktu lub z usługi powiązanej do pozyskania informacji o sytuacji ekonomicznej, aktywach i metodach produkcji posiadacza danych lub korzystaniu przez niego z produktu lub usługi powiązanej;

f) nie wykorzystuje otrzymanych danych w sposób, który niekorzystnie wpływa na bezpieczeństwo produktu skomunikowanego lub usługi powiązanej;

g) nie ignoruje szczególnych środków uzgodnionych z posiadaczem danych lub posiadaczem tajemnic przedsiębiorstwa zgodnie z art. 5 ust. 9 i nie zagraża poufności tajemnic przedsiębiorstwa;

h) nie uniemożliwia użytkownikowi będącemu konsumentem, w tym w drodze umowy, udostępniania innym osobom otrzymanych przez siebie danych.

Artykuł 7

Zakres obowiązków dzielenia się danymi przez przedsiębiorców z konsumentami i z innymi przedsiębiorcami

1. Obowiązki przewidziane w niniejszym rozdziale nie mają zastosowania do danych wygenerowanych w wyniku korzystania z wyprodukowanych lub zaprojektowanych produktów skomunikowanych lub z usług powiązanych dostarczonych przez mikroprzedsiębiorstwo lub małe przedsiębiorstwo, pod warunkiem że przedsiębiorstwo to nie ma przedsiębiorstwa partnerskiego ani przedsiębiorstwa powiązanego w rozumieniu art. 3 załącznika do zalecenia 2003/361/WE, które nie kwalifikuje się jako mikroprzedsiębiorstwo lub małe przedsiębiorstwo, a mikroprzedsiębiorstwo lub małe przedsiębiorstwo nie jest podwykonawcą, któremu zlecono wyprodukowanie lub zaprojektowanie produktu skomunikowanego lub też świadczenie usługi powiązanej.

   To samo ma zastosowanie do danych wygenerowanych w wyniku korzystania z produktów skomunikowanych wyprodukowanych lub z usług powiązanych dostarczonych przez przedsiębiorstwa, które kwalifikują się jako średnie przedsiębiorstwa zgodnie z art. 2 załącznika do zalecenia 2003/361/WE przez okres krótszy niż rok,, oraz do produktów skomunikowanych przez okres jednego roku od dnia wprowadzenia ich do obrotu przez średnie przedsiębiorstwo.

2. Postanowienie umowne, które ze szkodą dla użytkownika wyklucza stosowanie praw użytkownika przewidzianych w niniejszym rozdziale, stanowi odstępstwo od nich lub zmienia ich skutek, nie jest dla użytkownika wiążące.

Rozdział III
Obowiązki posiadaczy danych zobowiązanych do udostępniania danych zgodnie z prawem Unii

Artykuł 8

Warunki udostępniania danych przez posiadaczy danych odbiorcom danych

1. W przypadku gdy w relacjach między przedsiębiorcami posiadacz danych jest zobowiązany do udostępnienia danych odbiorcy danych na podstawie art. 5 lub innego mającego zastosowanie prawa Unii, lub prawa krajowego przyjętego zgodnie z prawem Unii, uzgadnia on z odbiorcą danych uzgodnienia dotyczące udostępnienia danych i robi to na sprawiedliwych, rozsądnych i niedyskryminujących zasadach oraz w przejrzysty sposób zgodnie z niniejszym rozdziałem i rozdziałem IV.

2. Postanowienie umowne dotyczące dostępu do danych i ich wykorzystywania lub odpowiedzialności i środków ochrony prawnej wobec naruszenia lub odstąpienia od obowiązków dotyczących danych nie jest wiążące, jeżeli stanowi nieuczciwe postanowienie umowne w rozumieniu art. 13 lub jeżeli na szkodę użytkownika wyłącza stosowanie praw użytkownika wynikających z rozdziału II, stanowi odstępstwo od tych praw lub zmienia ich skutek.

3. Przy udostępnianiu danych posiadacz danych nie rozróżnia uzgodnień dotyczących udostępniania danych dla porównywalnych kategorii odbiorców danych, w tym przedsiębiorstw partnerskich lub przedsiębiorstw powiązanych posiadacza danych. W przypadku gdy odbiorca danych uważa, że warunki, na których dane zostały mu udostępnione, są dyskryminujące, posiadacz danych bez zbędnej zwłoki przedstawia odbiorcy danych na jego uzasadniony wniosek informacje wykazujące, że nie doszło do dyskryminacji.

4. Posiadacz danych nie udostępnia danych odbiorcy danych, w tym na zasadzie wyłączności, chyba że użytkownik wystąpi z wnioskiem o to na podstawie rozdziału II.

5. Posiadacze danych i odbiorcy danych nie mają obowiązku przedstawiania żadnych informacji poza tymi, które są niezbędne do kontroli przestrzegania postanowień umownych uzgodnionych w celu udostępnienia danych lub obowiązków wynikających z niniejszego rozporządzenia lub innego mającego zastosowanie prawa Unii, lub prawa krajowego przyjętego zgodnie z prawem Unii.

6. O ile prawo Unii, w tym art. 4 ust. 6 i art. 5 ust. 9 niniejszego rozporządzenia, lub przepisy krajowe przyjęte zgodnie z prawem Unii nie stanowią inaczej, obowiązek udostępnienia danych odbiorcy danych nie zobowiązuje do ujawnienia tajemnic przedsiębiorstwa.

Artykuł 9

Rekompensata za udostępnienie danych

1. Wszelka rekompensata uzgodniona między posiadaczem danych a odbiorcą danych za udostępnienie danych w relacjach między przedsiębiorcami jest niedyskryminacyjna, zasadna i może obejmować marżę.

2. Przy uzgadnianiu wszelkiej rekompensaty posiadacz danych i odbiorca danych uwzględniają w szczególności:

   a) koszty poniesione w celu udostępnienia danych, w tym w szczególności koszty niezbędne do sformatowania danych, rozpowszechnienia danych za pomocą środków elektronicznych i ich przechowywania;

   b) inwestycje poczynione w zebranie i wytworzenie danych, w stosownym przypadku z uwzględnieniem, czy do pozyskania, wygenerowania lub zebrania przedmiotowych danych przyczyniły się inne strony.

3. Rekompensata, o której mowa w ust. 1, może także zależeć od ilości, formatu i charakteru danych.

4. W przypadku gdy odbiorcą danych jest MŚP lub niekomercyjna organizacja badawcza i gdy taki odbiorca danych nie ma przedsiębiorstw partnerskich ani przedsiębiorstw powiązanych, które nie kwalifikują się jako MŚP, uzgodniona rekompensata nie przekracza kosztów, o których mowa w ust. 2 lit. a).

5. Komisja przyjmuje wytyczne w sprawie obliczania zasadnej rekompensaty, uwzględniając stanowisko Europejskiej Rady ds. Innowacji w zakresie Danych o której mowa w art. 42.

6. Niniejszy artykuł nie stoi na przeszkodzie temu, by inne prawo Unii lub przepisy krajowe przyjęte zgodnie z prawem Unii wykluczały rekompensaty za udostępnienie danych lub przewidywały niższe wynagrodzenie.

7. Posiadacz danych przedstawia odbiorcy danych w sposób wystarczająco szczegółowy informacje określające podstawę obliczania rekompensaty, tak aby odbiorca danych mógł ocenić, czy spełnione zostały wymogi przewidziane w ust. 1—4.

Artykuł 10

Rozstrzyganie sporów

1. Użytkownicy, posiadacze danych i odbiorcy danych mają dostęp do organów rozstrzygania sporów, certyfikowanych zgodnie z ust. 5 niniejszego artykułu, na potrzeby rozstrzygania sporów na podstawie art. 4 ust. 3 i ust. 9 oraz art. 5 ust. 12, a także sporów w sprawie sprawiedliwych, rozsądnych i niedyskryminujących zasad i przejrzystego sposobu udostępnienia danych zgodnie z niniejszym rozdziałem i rozdziałem IV.

2. Organy rozstrzygania sporów informują zainteresowane strony o wysokości opłat lub o mechanizmach stosowanych do ustalania wysokości opłat, zanim strony te wystąpią o wydanie decyzji.

3. W przypadku sporów wniesionych do organu rozstrzygania sporów na podstawie art. 4 ust. 3 i ust. 9 oraz art. 5 ust. 12, jeżeli organ rozstrzygania sporów rozstrzygnie spór na korzyść użytkownika lub odbiorcy danych, posiadacz danych ponosi wszelkie opłaty nałożone przez organ rozstrzygania sporów i zwraca użytkownikowi lub odbiorcy danych wszelkie inne rozsądne koszty poniesione w związku z rozstrzygnięciem sporu. Jeżeli organ rozstrzygania sporów rozstrzygnie spór na korzyść posiadacza danych, użytkownik lub odbiorca danych nie są zobowiązani do zwrócenia opłat ani innych kosztów, które posiadacz danych poniósł lub ma ponieść w związku z rozstrzygnięciem sporu, chyba że organ rozstrzygania sporów uzna, że użytkownik lub odbiorca danych w oczywisty sposób działali w złej wierze.

4. Klienci i dostawcy usług przetwarzania danych mają dostęp do organów rozstrzygania sporów, certyfikowanych zgodnie z ust. 5 niniejszego artykułu, na potrzeby rozstrzygania sporów dotyczących naruszeń praw klientów i niewywiązania się z obowiązków przez dostawców usług przetwarzania danych, zgodnie z art. 23 do 31.

5. Państwo członkowskie, w którym ma siedzibę organ rozstrzygania sporów, na wniosek tego organu dokonuje jego certyfikacji, jeżeli organ ten wykazał, że spełnia wszystkie następujące warunki:

   a) jest bezstronny i niezależny oraz będzie wydawać decyzje zgodnie z jasnym, niedyskryminującym i sprawiedliwym regulaminem wewnętrznym;

   b) dysponuje niezbędną wiedzą ekspercką, w szczególności na temat sprawiedliwych, stosownych i niedyskryminujących zasad, w tym rekompensaty, oraz przejrzystego sposobu udostępniania danych, która to wiedza pozwala organowi na skuteczne ustalanie tych zasad;

   c) jest łatwo dostępny za pośrednictwem technologii łączności elektronicznej;

   d) ma możliwość przyjmowania decyzji w sposób szybki, skuteczny i oszczędny w co najmniej jednym języku urzędowym Unii.

6. Państwa członkowskie zgłaszają Komisji organy rozstrzygania sporów certyfikowane zgodnie z ust. 5. Komisja publikuje wykaz tych organów na specjalnej stronie internetowej i na bieżąco go aktualizuje.

7. Organy rozstrzygania sporów odmawiają rozpatrzenia wniosku o rozstrzygnięcie sporu, który został już wniesiony do innego organu rozstrzygania sporów, bądź do sądu lub trybunału państwa członkowskiego.

8. Organy rozstrzygania sporów dają stronom możliwość wyrażenia, w rozsądnym terminie, swojego stanowiska w sprawach wniesionych przez te strony do tych organów. W tym kontekście każda strona sporu otrzyma stanowiska drugiej strony sporu oraz wszelkie opinie ekspertów. Stronom zapewnia się możliwość ustosunkowania się do tych stanowisk i opinii.

9. Organy rozstrzygania sporów przyjmują decyzję w skierowanych do nich sprawach w ciągu 90 dni od otrzymania wniosku zgodnie z ust. 1 i 4. Decyzje te sporządza się na piśmie lub na trwałym nośniku i opatruje uzasadnieniem.

10. Organy rozstrzygania sporów sporządzają i podają do wiadomości publicznej roczne sprawozdania z działalności. Roczne sprawozdania zawierają w szczególności następujące informacje ogólne:

    a) zbiorcze podsumowanie wyników sporów;

    b) średni czas rozstrzygania sporów;

    c) najczęstsze powody sporów.

11. Aby ułatwić wymianę informacji i najlepszych praktyk, organ rozstrzygania sporów może zdecydować o dodaniu do sprawozdania, o którym mowa w ust. 10, zaleceń dotyczących metod zapobiegania problemom lub ich rozwiązywania.

12. Decyzja organu rozstrzygającego spory jest wiążąca dla stron wyłącznie wtedy, gdy strony wyraźnie zgodziły się na jej wiążący charakter przed rozpoczęciem postępowania w sprawie rozstrzygnięcia sporu.

13. Niniejszy artykuł nie wpływa na prawa stron do dochodzenia skutecznego środka prawnego przed sądem lub trybunałem państwa członkowskiego.

Artykuł 11

Techniczne środki ochrony i przepisy dotyczące nieuprawnionego wykorzystywania lub ujawniania danych

1. Posiadacz danych może stosować odpowiednie techniczne środki ochrony, w tym inteligentne umowy i szyfrowanie, aby zapobiec nieuprawnionemu dostępowi do danych, w tym metadanych, i zapewnić zgodność z art. 5, 6, 8 i 9 oraz uzgodnionymi postanowieniami umownymi dotyczącymi udostępniania danych. Takie techniczne środki ochrony nie powodują różnego traktowania odbiorców danych ani nie ograniczają prawa użytkownika do uzyskania kopii danych, pobrania bądź wykorzystania danych, dostępu do danych lub dostarczenia danych osobom trzecim zgodnie z art. 5 ani jakiegokolwiek prawa osoby trzeciej wynikającego z prawa Unii lub prawa krajowego przyjętego zgodnie z prawem Unii. Użytkownicy, osoby trzecie lub odbiorcy danych nie zmieniają ani nie usuwają takich technicznych środków ochrony, chyba że posiadacz danych wyraził na to zgodę.

2. W przypadkach, o których mowa w ust. 3, osoba trzecia lub odbiorca danych na żądanie posiadacza danych oraz w stosownych przypadkach, jeżeli nie są oni tą samą osobą, posiadacza tajemnicy przedsiębiorstwa lub użytkownika:

a) usuwają dane udostępnione przez posiadacza danych oraz wszelkie ich kopie;

b) zaprzestają produkcji, oferowania, wprowadzania do obrotu lub wykorzystywania towarów, danych wywnioskowanych lub usług wytworzonych na podstawie wiedzy pozyskanej dzięki takim danym lub przywozu, wywozu lub magazynowania do tych celów towarów naruszających prawo oraz niszczą wszelkie towary naruszające prawo, w przypadku gdy istnieje poważne ryzyko, że niezgodne z prawem wykorzystywanie tych danych spowoduje znaczną szkodę dla posiadacza danych, posiadacza tajemnicy przedsiębiorstwa lub użytkownika, lub gdy taki środek nie byłby nieproporcjonalny w świetle interesów posiadacza danych, posiadacza tajemnicy przedsiębiorstwa lub użytkownika;

c) informują użytkownika o nieuprawnionym wykorzystaniu lub ujawnieniu danych oraz o środkach zastosowanych, aby położyć kres nieuprawnionemu wykorzystywaniu lub ujawnianiu danych;

d) rekompensują szkodę stronie, która ją poniosła w wyniku niewłaściwego wykorzystania lub ujawnienia takich danych udostępnionych lub wykorzystanych niezgodnie z prawem.

3. Ust. 2 ma zastosowanie, gdy osoba trzecia lub odbiorca danych:

a) w celu pozyskania danych przedstawili posiadaczowi danych nieprawdziwe informacje, zastosowali środki wprowadzające w błąd lub środki przymusu lub wykorzystali lukę w infrastrukturze technicznej posiadacza danych mającą chronić dane;

b) wykorzystali udostępnione dane w nieuprawnionych celach, w tym do stworzenia konkurencyjnego produktu skomunikowanego w rozumieniu art. 6 ust. 2 lit. e);

c) niezgodnie z prawem ujawnili dane innej osobie;

d) nie utrzymali środków technicznych i organizacyjnych uzgodnionych zgodnie z art. 5 ust. 9;

e) bez zgody posiadacza danych zmienili lub usunęli techniczne środki ochrony stosowane przez posiadacza danych zgodnie z ust. 1 niniejszego artykułu.

4. Ustęp 2 ma również zastosowanie, gdy użytkownik zmienia lub usuwa techniczne środki ochrony zastosowane przez posiadacza danych lub nie utrzymuje środków technicznych i organizacyjnych zastosowanych przez użytkownika w celu ochrony tajemnic przedsiębiorstwa w porozumieniu z posiadaczem danych lub, jeżeli nie jest tą samą osobą, z posiadaczem tajemnicy przedsiębiorstwa, a także gdy inna osoba otrzymała dane od użytkownika w wyniku naruszenia niniejszego rozporządzenia.

5. W przypadku gdy odbiorca danych narusza art. 6 ust. 2 lit. a) lub b), użytkownicy mają takie same prawa jak posiadacze danych na podstawie ust. 2 niniejszego artykułu.

Artykuł 12

Zakres obowiązków posiadaczy danych zobowiązanych zgodnie z prawem Unii do udostępniania danych

1. Niniejszy rozdział ma zastosowanie, w przypadku gdy w stosunkach między przedsiębiorcami posiadacz danych jest zobowiązany do udostępnienia danych odbiorcy danych na podstawie art. 5 lub mającego zastosowanie prawa Unii, lub przepisów krajowych przyjętych zgodnie z prawem Unii.

2. Postanowienie umowne zawarte w umowie w sprawie dzielenia się danymi, które ze szkodą dla jednej ze stron lub w stosownym przypadku ze szkodą dla użytkownika wyłącza stosowanie niniejszego rozdziału, stanowi odstępstwo od niego lub zmienia jego skutki, nie jest dla tej strony wiążące.

Rozdział IV

Nieuczciwe postanowienia umowne między przedsiębiorstwami dotyczące dostępu do danych i ich wykorzystywania

Artykuł 13

Nieuczciwe postanowienia umowne nałożone jednostronnie na inne przedsiębiorstwo

1. Postanowienie umowne dotyczące dostępu do danych i ich wykorzystywania lub odpowiedzialności i środków ochrony prawnej wobec naruszenia lub odstąpienia od obowiązków dotyczących danych i nałożone jednostronnie na inne przedsiębiorstwo nie jest dla tego innego przedsiębiorstwa wiążące, jeżeli postanowienie to jest nieuczciwe.

2. Postanowienie umowne nie jest uznawane za nieuczciwe, jeżeli stanowi odzwierciedlenie bezwzględnie obowiązujących przepisów prawa Unii, które miałyby zastosowanie, gdyby przedmiotowej sprawy nie regulowały postanowienia umowne.

3. Postanowienie umowne jest nieuczciwe, jeżeli cechuje się tym, że jego stosowanie rażąco odbiega od dobrej praktyki handlowej w zakresie dostępu do danych i ich wykorzystywania, w przeciwieństwie do zasady dobrej wiary i uczciwego obrotu.

4. W szczególności postanowienie umowne jest nieuczciwe do celów ust. 3, jeżeli jego celem lub skutkiem jest:

a) wyłączenie lub ograniczenie odpowiedzialności strony, która jednostronnie narzuciła postanowienie, za czyny umyślne lub wynikające z rażącego niedbalstwa;

b) wyłączenie środków ochrony prawnej dostępnych stronie, na którą jednostronnie narzucono postanowienie, w przypadku niewykonania zobowiązań umownych lub wyłączenie odpowiedzialności strony, która jednostronnie narzuciła postanowienie, w przypadku naruszenia tych zobowiązań;

c) przyznanie stronie, która jednostronnie narzuciła postanowienie, wyłącznego prawa do ustalania, czy dostarczone dane są zgodne z umową, lub wyłącznego prawa do interpretowania postanowienia umownego.

5. Domniemywa się, że postanowienie umowne jest nieuczciwe do celów ust. 3, jeżeli jego celem lub skutkiem jest:

a) niewłaściwe ograniczenie środków ochrony prawnej w przypadku niewykonania zobowiązań umownych lub niewłaściwe ograniczenie odpowiedzialności w przypadku naruszenia tych zobowiązań, lub rozszerzenie odpowiedzialności przedsiębiorstwa, na które jednostronnie narzucone zostało postanowienie;

b) umożliwienie stronie, która jednostronnie narzuciła postanowienie, dostępu do danych drugiej umawiającej się strony i ich wykorzystania w sposób znacząco szkodliwy dla uzasadnionych interesów drugiej umawiającej się strony, w szczególności gdy takie dane zawierają szczególnie chronione dane handlowe lub są chronione tajemnicami przedsiębiorstwa lub prawami własności intelektualnej**;**

c) uniemożliwienie stronie, na którą jednostronnie nałożono postanowienie, wykorzystywania danych dostarczonych lub wygenerowanych przez tę stronę w okresie obowiązywania umowy lub ograniczenie wykorzystywania takich danych w takim stopniu, że strona ta nie jest uprawniona do wykorzystywania takich danych, pobierania ich, uzyskiwania do nich dostępu, kontrolowania ich lub wykorzystywania ich wartości w odpowiedni sposób;

d) uniemożliwienie stronie, na którą jednostronnie narzucono postanowienie, rozwiązania umowy w rozsądnym terminie;

e) uniemożliwienie stronie, na którą jednostronnie narzucono postanowienie, uzyskania kopii danych dostarczonych lub wygenerowanych przez tę stronę w okresie obowiązywania umowy lub w rozsądnym okresie po jego rozwiązaniu;

f) umożliwienie stronie, która jednostronnie narzuciła postanowienie, rozwiązania umowy ze zbyt krótkim terminem wypowiedzenia, biorąc pod uwagę rozsądną możliwość drugiej umawiającej się strony zmiany usługi na alternatywną i porównywalną oraz szkodę finansową spowodowaną takim rozwiązaniem, chyba że istnieją ku temu poważne podstawy;

g) umożliwienie stronie, która jednostronnie narzuciła postanowienie, istotnej zmiany ceny ustalonej w umowie lub jakiegokolwiek innego istotnego warunku związanego z charakterem, formatem, jakością lub ilością danych podlegających dzieleniu się, bez ważnej przyczyny określonej w umowie i bez prawa drugiej strony do rozwiązania umowy w razie takiej zmiany.

Akapit pierwszy lit. g)e nie wpływa na postanowienia pozwalające stronie, która jednostronnie narzuciła postanowienie, zastrzec sobie prawo do jednostronnej zmiany postanowień umowy na czas nieokreślony, pod warunkiem że w umowie tej określona została ważna przyczyna dla takich jednostronnych zmian, o której strona, która jednostronnie narzuciła postanowienie, jest zobowiązana w rozsądnym terminie poinformować drugą umawiającą się stronę, a druga umawiająca się strona może rozwiązać umowę w razie zmiany bez ponoszenia kosztów.

6. Postanowienie umowne uważa się za jednostronnie narzucone w rozumieniu niniejszego artykułu, jeżeli zaproponowała je jedna umawiająca się strona, a druga umawiająca się strona nie była w stanie wpłynąć na jego treść pomimo próby negocjacji tej treści. Ciężar udowodnienia, że postanowienie umowne nie zostało jednostronnie narzucone, spoczywa na umawiającej się stronie, która zaproponowała to postanowienie. Umawiająca się strona, która zaproponowała sporne postanowienie, nie może twierdzić, że jest to nieuczciwe postanowienie umowne.

7. W przypadku gdy nieuczciwe postanowienie umowne można oddzielić od pozostałych postanowień umowy, pozostałe postanowienia pozostają wiążące.

8. Niniejszy artykuł nie ma zastosowania do postanowień umownych określających główny przedmiot umowy lub do relacji ceny do dostarczonych w zamian danych.

9. Strony umowy objętej ust. 1 nie wyłączają stosowania niniejszego artykułu, nie odstępują od niego ani nie zmieniają jego skutków.

Rozdział V
Udostępnianie danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu i organom Unii na podstawie wyjątkowej potrzeby

Artykuł 14

Obowiązek udostępnienia danych na podstawie wyjątkowej potrzeby

W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii wykażą wyjątkową potrzebę, o której mowa w art. 15, wykorzystania określonych danych – w tym odpowiednich metadanych niezbędnych do interpretacji i wykorzystania tych danych – w celu wykonania swoich ustawowych obowiązków realizowanych w interesie publicznym, posiadacze danych będący osobami prawnymi, którzy posiadają te dane, inni niż organy sektora publicznego, udostępniają je w odpowiedzi na należycie uzasadniony wniosek.

Artykuł 15

Wyjątkowa potrzeba wykorzystania danych

1. Wyjątkowa potrzeba wykorzystania określonych danych w rozumieniu niniejszego rozdziału jest ograniczona w czasie i zakresie i uznaje się, że istnieje wyłącznie w następujących okolicznościach:

   a) gdy żądane dane są niezbędne do zareagowania na niebezpieczeństwo publiczne, a organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii nie są w stanie skutecznie i na czas pozyskać takich danych w alternatywny sposób na równoważnych warunkach;

   b) w okolicznościach nieobjętych lit. a) i wyłącznie w przypadku danych nieosobowych, gdy:

      (i) organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii działają na podstawie prawa Unii lub prawa krajowego i zidentyfikowały konkretne dane, których brak uniemożliwia im wykonanie konkretnego zadania realizowanego w interesie publicznym, które jest wyraźnie przewidziane prawem, takiego jak tworzenie statystyki publicznej lub łagodzenie niebezpieczeństwa publicznego lub przywracanie stanu wyjściowego po jego wystąpieniu; oraz

(ii) organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii wyczerpały wszystkie inne dostępne im sposoby pozyskania takich danych, w tym zakup danych nieosobowych na rynku poprzez zaoferowanie stawek rynkowych, powołanie się na istniejące obowiązki udostępniania danych lub poprzez przyjęcie nowych środków ustawodawczych, które mogłyby zagwarantować dostępność danych na czas.

2. Ust. 1 lit. b) nie ma zastosowania do mikroprzedsiębiorstw ani do małych przedsiębiorstw.

3. Obowiązek wykazania, że organ sektora publicznego nie był w stanie pozyskać danych nieosobowych poprzez ich zakup na rynku, nie ma zastosowania, w przypadku gdy konkretnym zadaniem realizowanym w interesie publicznym jest tworzenie statystyki publicznej i gdy na zakup danych nie zezwala prawo krajowe.

Artykuł 16

Związek z innymi obowiązkami udostępniania danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu i organom Unii

1. Niniejszy rozdział nie wpływa na obowiązki określone w prawie Unii lub prawie krajowym w zakresie sprawozdawczości, stosowania się do wniosków o dostęp do informacji lub wykazywania i weryfikacji przestrzegania obowiązków prawnych.

2. Niniejszy rozdział nie ma zastosowania do organów sektora publicznego, Komisji, Europejskiego Banku Centralnego ani organów Unii, gdy wykonują one działania w zakresie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych lub wykonywania sankcji karnych ani do administracji celnej lub podatkowej. Niniejszy rozdział nie wpływa na mające zastosowanie prawo Unii i prawo krajowe dotyczące zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych lub wykonywania sankcji karnych lub kar administracyjnych ani administracji celnej lub podatkowej.

Artykuł 17

Wnioski o udostępnienie danych

1. Występując z wnioskiem o dane na podstawie art. 14, organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii:

   a) określają, jakie dane, w tym odpowiednie metadane niezbędne do interpretacji i wykorzystania tych danych, są potrzebne;

   b) wykazują, że spełnione zostały warunki wyjątkowej potrzeby, o której mowa w art. 15 i na podstawie której występuje się z wnioskiem o dane;

   c) wyjaśniają cel wniosku, planowane wykorzystanie żądanych danych, w tym, w stosownym przypadku, przez osobę trzecią zgodnie z ust. 4 niniejszego artykułu, czas tego wykorzystywania oraz w stosownym przypadku sposób, w jaki przetwarzanie danych osobowych ma odpowiedzieć na wyjątkową potrzebę;

d) w miarę możliwości określają, kiedy można się spodziewać, że dane zostaną usunięte przez wszystkie strony, które mają do nich dostęp;

e) uzasadniają wybór posiadacza danych, do którego skierowany jest wniosek;

f) wymieniają inne organy sektora publicznego, lub Komisję, Europejski Bank Centralny lub organy Unii oraz osoby trzecie, z którymi żądane dane mają być dzielone;

g) jeżeli żądanymi danymi są dane osobowe, określają niezbędne i proporcjonalne środki techniczne i organizacyjne służące wdrożeniu zasad ochrony danych i niezbędnych zabezpieczeń, takich jak poziom agregacji lub pseudonimizacji, oraz czy posiadacz danych może dokonać pseudonimizacji przed udostępnieniem danych;

h) podają podstawę prawną konkretnego zadania realizowanego w interesie publicznym organu publicznego, Komisji, Europejskiego Banku Centralnego lub organu Unii, w związku z którym występuje się z wnioskiem o dane;

i) określają termin, w którym dane mają zostać udostępnione oraz termin, o którym mowa w art. 18 ust. 2, w którym posiadacz danych może odmówić lub wnosić o zmianę wniosku;

j) dokładają wszelkich starań, aby zastosowanie się do wniosku o dane nie skutkowało odpowiedzialnością posiadacza danych za naruszenie prawa Unii lub prawa krajowego.

2. Wniosek o dane złożony na podstawie ust. 1 niniejszego artykułu:

a) jest składany na piśmie i sformułowany jasnym, zwięzłym i prostym językiem zrozumiałym dla posiadacza danych;

b) zawiera szczegóły dotyczące rodzaju żądanych danych i odnosi się do danych, nad którymi posiadacz danych ma kontrolę w momencie składania wniosku;

c) jest proporcjonalny do wyjątkowej potrzeby i należycie uzasadniony w odniesieniu do szczegółowości i ilości żądanych danych oraz częstotliwości dostępu do żądanych danych;

d) respektuje prawnie uzasadnione cele posiadacza danych, w tym obowiązek zapewnienia ochrony tajemnic przedsiębiorstwa, zgodnie z art. 19 ust. 3, oraz uwzględniając koszty i działania wymagane do udostępnienia danych;

e) dotyczy danych nieosobowych i zawiera żądanie udostępnienia spseudonimizowanych danych osobowych wyłącznie wtedy, gdy wykazano, że data nieosobowe nie są wystarczające w celu odpowiedzi na wyjątkową potrzebę wykorzystania danych, zgodnie z art. 15 ust. 1 lit. a), i określa środki techniczne i organizacyjne, które zostaną zastosowane, aby chronić te dane osobowe;

f) informuje posiadacza danych o karach nakładanych na podstawie art. 40 przez właściwy organ wyznaczony zgodnie z w art. 37 w przypadku niezastosowania się do wniosku;

g) w przypadku gdy wniosek jest złożony przez organ sektora publicznego, zostaje przekazany koordynatorowi danych, o którym mowa w art. 37, w państwie członkowskim, w którym siedzibę ma organ sektora publicznego, a organ ten bez zbędnej zwłoki podaje wniosek do wiadomości publicznej w internecie, chyba że koordynator danych uzna takie podanie do wiadomości za zagrożenie dla bezpieczeństwa publicznego;

h) w przypadku gdy wniosek jest złożony przez Komisję, Europejski Bank Centralny lub organ Unii bez zbędnej zwłoki podają one swoje wnioski do wiadomości publicznej w internecie;

i) w przypadku gdy dotyczy danych osobowych, bez zbędnej zwłoki zostaje o nim powiadomiony organ nadzorczy odpowiedzialny za monitorowanie stosowania rozporządzenia (UE) 2016/679 w państwie członkowskim, w którym siedzibę ma organ sektora publicznego.

Europejski Bank Centralny i organy Unii informują Komisję o swoich wnioskach.

3. Organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii nie udostępniają danych pozyskanych na podstawie niniejszego rozdziału do ponownego wykorzystania zdefiniowanego w art. 2 pkt 2rozporządzenia (UE) 2022/868 lub art. 2 pkt 11 dyrektywy (UE) 2019/1024. Rozporządzenie (UE) 2022/868 i dyrektywa (UE) 2019/1024 nie mają zastosowania do danych będących w posiadaniu organów sektora publicznego i pozyskanych na podstawie niniejszego rozdziału.

4. Ust. 3 niniejszego artykułu nie uniemożliwia organowi sektora publicznego ani Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii wymiany danych pozyskanych na podstawie niniejszego rozdziału z innym organem sektora publicznego, Komisją, Europejskim Bankiem Centralnym lub organem Unii w celu wypełnienia zadań, o których mowa w art. 15, określonych we wniosku zgodnie z ust. 1 lit. f) niniejszego artykułu, ani udostępnienia danych osobie trzeciej, w przypadku gdy zleciły tej osobie trzeciej – w drodze publicznie dostępnej umowy – kontrole techniczne lub inne funkcje. Do takich osób trzecich zastosowanie mają obowiązki nałożone na organy sektora publicznego na podstawie art. 19, w szczególności zabezpieczenia służące ochronie tajemnic przedsiębiorstwa. W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii przesyłają lub udostępniają dane na podstawie niniejszego ustępu, bez zbędnej zwłoki powiadamiają o tym posiadacza danych, od którego otrzymały dane.

5. W przypadku gdy posiadacz danych uzna, że naruszone zostały prawa przysługujące mu na podstawie niniejszego rozdziału poprzez przesłanie lub udostępnienie danych, może złożyć skargę do właściwego organu, wyznaczonego zgodnie z art. 37, w państwie członkowskim, w którym posiadacz danych ma siedzibę.

6. Na podstawie niniejszego artykułu Komisja opracowuje wzór wniosku.

Artykuł 18

Stosowanie się do wniosków o dane

1. Posiadacz danych otrzymujący wniosek o udostępnienie danych na podstawie niniejszego rozdziału bez zbędnej zwłoki udostępnia dane organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii, które wystąpiły z wnioskiem, uwzględniając niezbędne środki techniczne, organizacyjne i prawne.

2. Bez uszczerbku dla określonych w prawie Unii lub prawie krajowym szczególnych potrzeb w zakresie dostępności danych posiadacz danych może odmówić zastosowania się do wniosku o udostępnienie danych przewidzianego w niniejszym rozdziale lub wystąpić o jego zmianę bez zbędnej zwłoki i w żadnym razie nie później niż pięć dni roboczych od otrzymania wniosku o dane niezbędne do zareagowania na niebezpieczeństwo publiczne oraz bez zbędnej zwłoki i w żadnym razie nie później niż 30 dni roboczych od otrzymania takiego wniosku w innych przypadkach występowania wyjątkowej potrzeby, powołując się na jeden z następujących powodów:

   a) posiadacz danych nie ma kontroli nad żądanymi danymi;

   b) podobny wniosek w tym samym celu złożyły wcześniej inny organ sektora publicznego lub Komisja, Europejski Bank Centralny lub organ Unii, a posiadacza danych nie powiadomiono o usunięciu danych zgodnie z art. 19 ust. 1 lit. c);

   c) wniosek nie spełnia warunków określonych w art. 17 ust. 1 i 2.

3. Jeżeli posiadacz danych postanowi odmówić zastosowania się do wniosku lub wystąpić o jego zmianę zgodnie z ust. 2 lit. b), wskazuje tożsamość organu sektora publicznego lub Komisji, Europejskiego Banku Centralnego lub organu Unii, które wcześniej złożyły wniosek w tym samym celu.

4. W przypadku gdy żądane dane zawierają dane osobowe, posiadacz danych odpowiednio anonimizuje dane, chyba że zastosowanie się do wniosku o udostępnienie danych organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii wymaga ujawnienia danych osobowych. W takich przypadkach posiadacz danych pseudonimizuje dane.

5. W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii chcą zaskarżyć odmowę dostarczenia żądanych danych przez posiadacza danych lub gdy posiadacz danych chce zaskarżyć wniosek, a sprawy nie da się rozstrzygnąć poprzez odpowiednią zmianę wniosku, zostaje ona wniesiona do właściwego organu wyznaczonego zgodnie z art. 37, w państwie członkowskim, w którym posiadacz danych ma siedzibę.

Artykuł 19

Obowiązki organów sektora publicznego, Komisji, Europejskiego Banku Centralnego i organów Unii

1. Organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii, które otrzymały dane zgodnie z wnioskiem złożonym na podstawie art. 14:

   a) nie wykorzystują danych w sposób niezgodny z celem, w którym o nie wystąpiono;

b) wdrożyły środki techniczne i organizacyjne chroniące poufność i integralność żądanych danych oraz bezpieczeństwo przekazywania danych, w szczególności danych osobowych, oraz chronią prawa i wolności osób, których dane dotyczą;

c) usuwają dane, gdy tylko przestaną one być niezbędne do określonego celu, i bez zbędnej zwłoki informują o ich usunięciu posiadacza danych oraz osoby fizyczne lub organizacje, które otrzymały dane na podstawie art. 21 ust. 1, chyba że prawo Unii lub prawo krajowe dotyczące publicznego dostępu do dokumentów wymaga archiwizacji danych w kontekście obowiązków dotyczących przejrzystości.

2. Organ sektora publicznego, Komisja, Europejski Bank Centralny, organ Unii lub osoba trzecia otrzymujące dane na podstawie niniejszego rozdziału:

a) nie wykorzystują danych lub informacji o sytuacji ekonomicznej, aktywach oraz metodach produkcji lub działalności posiadacza danych, aby opracować lub udoskonalić produkt skomunikowany lub usługę powiązaną konkurujące z produktem skomunikowanym lub usługą powiązaną posiadacza danych;

b) nie dzielą się danymi z inną osobą trzecią w jakimkolwiek z celów, o których mowa w lit. a).

3. Ujawnienie tajemnicy przedsiębiorstwa organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii jest wymagane wyłącznie w zakresie, w jakim jest to bezwzględnie konieczne do osiągnięcia celu wniosku złożonego na podstawie art. 15. W takim przypadku posiadacz danych lub, jeżeli nie jest tą samą osobą, posiadacz tajemnicy przedsiębiorstwa identyfikują dane chronione, w tym w stosownych metadanych, jako tajemnice przedsiębiorstwa. Przed ujawnieniem tajemnic przedsiębiorstwa organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii stosują wszelkie niezbędne i odpowiednie środki techniczne i organizacyjne, aby chronić poufność tajemnic przedsiębiorstwa, w tym w stosownym przypadku używają modelowych postanowień umownych, norm technicznych oraz kodeksów postępowania.

4. Organ sektora publicznego, Komisja, Europejski Banki Centralny lub organ Unii odpowiadają za bezpieczeństwo otrzymanych danych.

Artykuł 20

Rekompensata w przypadkach wyjątkowej potrzeby

1. Posiadacze danych inni niż mikroprzedsiębiorstwa i małe przedsiębiorstwa nieodpłatnie udostępniają dane niezbędne do zareagowania na niebezpieczeństwo publiczne na podstawie art. 15 ust. 1 lit. a). Organ sektora publicznego, Komisja, Europejski Banki Centralny lub organ Unii, które otrzymały dane, zapewniają publiczne uznanie posiadaczowi danych, jeżeli posiadacz danych o to wystąpi.

2. Posiadacz danych jest uprawniony do zasadnej rekompensaty za udostępnienie danych zgodnie z wnioskiem złożonym na podstawie art. 15 ust. 1 lit. b). Rekompensata taka pokrywa koszty techniczne i organizacyjne poniesione w celu zastosowania się do wniosku, w tym w stosownym przypadku koszty anonimizacji, pseudonimizacji, agregacji i dostosowania technicznego, powiększone o rozsądną marżę. Na żądanie organu sektora publicznego, Komisji, Europejskiego Banku Centralnego lub organu Unii, posiadacz danych przedstawia informacje o podstawie obliczenia kosztów i rozsądnej marży.

3. Ust. 2 ma zastosowanie także wtedy, gdy o rekompensatę za udostępnienie danych występują mikroprzedsiębiorstwo lub małe przedsiębiorstwo.

4. Posiadacze danych nie mogą domagać się rekompensaty za udostępnienie danych zgodnie z wnioskiem wystosowanym na podstawie art. 15 ust. 1 lit. b), jeżeli konkretnym zadaniem realizowanym w interesie publicznym jest tworzenie statystyki publicznej i jeżeli prawo krajowe nie zezwala na sprzedaż danych. Państwa członkowskie powiadamiają Komisję, jeżeli prawo krajowe nie zezwala na sprzedaż danych na potrzeby tworzenia statystyki publicznej.

5. W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii nie zgadzają się z wysokością rekompensaty żądanej przez posiadacza danych, mogą złożyć skargę do właściwego organu wyznaczonego zgodnie z art. 37, w państwie członkowskim, w którym posiadacz danych ma siedzibę.

Artykuł 21

Dzielenie się danymi pozyskanymi w ramach wyjątkowej potrzeby z organizacjami badawczymi lub urzędami statystycznymi

1. Organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii są uprawnione do dzielenia się danymi otrzymanymi w ramach niniejszego rozdziału:

   a) z osobami fizycznymi lub organizacjami na potrzeby prowadzenia badań naukowych lub analiz zgodnych z celem, w którym wystąpiono o dane; lub

   b) z krajowymi urzędami statystycznymi i Eurostatem do celów tworzenia statystyki publicznej.

2. Osoby fizyczne lub organizacje otrzymujące dane na podstawie ust. 1 prowadzą działalność o charakterze niekomercyjnym lub w kontekście misji interesu publicznego uznanej w prawie Unii lub w prawie krajowym. Nie zaliczają się do nich organizacje znajdujące się pod znacznym wpływem przedsiębiorstw komercyjnych, który mógłby skutkować preferencyjnym dostępem do wyników badań.

3. Osoby fizyczne lub organizacje otrzymujące dane na podstawie ust. 1 niniejszego artykułu przestrzegają tych samych obowiązków, które mają zastosowanie do organów sektora publicznego, Komisji, Europejskiego Banku Centralnego lub organów Unii na podstawie art. 17 ust. 3 i art. 19.

4. Niezależnie od art. 19 ust. 1 lit. c) osoby fizyczne lub organizacje otrzymujące dane na podstawie ust. 1 niniejszego artykułu mogą zachować dane otrzymane w celu, w którym o nie wystąpiono, maksymalnie przez sześć miesięcy po usunięciu danych przez organy sektora publicznego, Komisję, Europejski Bank Centralny i organy Unii.

5. W przypadku gdy organ sektora publicznego, Komisja, Europejski Bank Centralny lub organ Unii zamierzają przesłać lub udostępnić dane na podstawie ust. 1 niniejszego artykułu, bez zbędnej zwłoki powiadamiają o tym posiadacza danych, od którego otrzymano dane, podając dane identyfikacyjne i kontaktowe organizacji lub osoby fizycznej otrzymujących dane, cel przesłania lub udostępnienia danych, okres, przez który dane będą wykorzystywane, oraz zastosowane techniczne i organizacyjne środki ochrony, w tym jeżeli w grę wchodzą dane osobowe lub tajemnice przedsiębiorstwa. W przypadku gdy posiadacz danych nie zgadza się na przesłanie lub udostępnienie danych, może złożyć skargę do właściwego organu wyznaczonego zgodnie z art. 37, w państwie członkowskim, w którym posiadacz danych ma siedzibę.

Artykuł 22

Wzajemna pomoc i współpraca transgraniczna

1. Organy sektora publicznego, Komisja, Europejski Bank Centralny i organy Unii współpracują ze sobą i udzielają sobie wzajemnie pomocy w celu spójnego wdrożenia niniejszego rozdziału.

2. Dane wymienione w kontekście pomocy, o którą wystąpiono i której udzielono na podstawie ust. 1, nie są wykorzystywane w sposób niezgodny z celem, w którym o nie wystąpiono.

3. W przypadku gdy organ sektora publicznego zamierza wystąpić z wnioskiem o dane do posiadacza danych mającego siedzibę w innym państwie członkowskim, najpierw powiadamia o tym zamiarze właściwy organ wyznaczony zgodnie z art. 37 w tym państwie członkowskim. Wymóg ten ma zastosowanie także do wniosków wystosowywanych przez Komisję, Europejski Bank Centralny i organy Unii. Właściwy organ państwa członkowskiego, w którym posiadacz danych ma siedzibę, bada wniosek.

4. Po zbadaniu wniosku w świetle wymogów art. 17 stosowny właściwy organ bez zbędnej zwłoki podejmuje jedno z następujących działań:

   a) przesyła wniosek posiadaczowi danych i w stosownym przypadku doradza organowi sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu lub organowi Unii, które występują z wnioskiem, w sprawie potrzeby, jeżeli taka występuje, o współpracę z organami sektora publicznego w państwie członkowskim, w którym posiadacz danych ma siedzibę, w celu zmniejszenia obciążeń administracyjnych spoczywających na posiadaczu danych w kwestii zastosowania się do wniosku;

   b) z należycie uzasadnionych powodów, zgodnie z niniejszym rozdziałem, odrzuca wniosek.

   W stosownych przypadkach, organ sektora publicznego, który wystąpił z wnioskiem, Komisja, Europejski Bank Centralny i organ Unii biorą pod uwagę opinię i powody przedstawione przez odpowiedni właściwy organ zgodnie z akapitem pierwszym, przed podjęciem wszelkich dalszych działań, takich jak ponowne złożenie wniosku.

Rozdział VI
Zmiana dostawcy usług przetwarzania danych

Artykuł 23

Usuwanie przeszkód w skutecznej zmianie dostawcy

Dostawcy usług przetwarzania danych stosują środki przewidziane w art. 25, 26, 27, 29 i 30, aby umożliwić klientom zmianę usługi przetwarzania danych na usługę tego samego typu świadczoną przez innego dostawcę usług przetwarzania danych, lokalną infrastrukturę ICT lub w stosownym przypadku korzystanie z usług kilku dostawców usług przetwarzania danych równocześnie.
W szczególności dostawcy usług przetwarzania danych nie stawiają przeszkód przedkomercyjnych, handlowych, technicznych, umownych i organizacyjnych i je usuwają, jeżeli utrudniają one klientom:

a) rozwiązanie umowy o świadczenie usługi przetwarzania danych po upływie maksymalnego okresu wypowiedzenia i pomyślną finalizację procesu zmiany dostawcy, zgodnie z art. 25;

b) zawarcie nowych umów z innym dostawcą usług przetwarzania danych obejmujących usługi tego samego typu;

c) przeniesienie danych eksportowalnych i aktywów cyfrowych klienta do innego dostawcy usług przetwarzania danych lub do lokalnej infrastruktury ICT, w tym po skorzystaniu z oferty na poziomie bezpłatnym;

d) zgodnie z art. 24 uzyskanie równoważności funkcjonalnej w ramach korzystania z nowej usługi przetwarzania danych w środowisku informatycznym innego dostawcy obejmującym usługę tego samego typu;

e) oddzielenie, jeżeli jest to technicznie możliwe, usług przetwarzania danych, o których mowa w art. 30 ust. 1, od innych usług przetwarzania danych świadczonych przez dostawcę usługi przetwarzania danych.

Artykuł 24

Zakres obowiązków technicznych

Obowiązki dostawców usług przetwarzania danych określone w art. 23, 25, 29, 30 i 34 mają zastosowanie wyłącznie do usług, umów lub praktyk handlowych wyjściowego dostawcy usług przetwarzania danych.

Artykuł 25

Postanowienia umowne dotyczące zmiany dostawcy

1. Prawa klienta i obowiązki dostawcy usługi przetwarzania danych w odniesieniu do zmiany dostawcy takich usług lub w stosownym przypadku do przeniesienia do lokalnej infrastruktury ICT zostaną jasno określone w umowie zawartej na piśmie. Dostawca usług przetwarzania danych udostępnia taką umowę klientowi przed podpisaniem w sposób umożliwiający klientowi jej przechowywanie i reprodukowanie.

2. Bez uszczerbku dla dyrektywy (UE) 2019/770 w umowie, o której mowa w ust. 1 niniejszego artykułu znajdują się co najmniej następujące elementy:

   a) postanowienia umowne umożliwiające klientowi na wniosek zmianę dostawcy usług przetwarzania danych na innego dostawcę usług przetwarzania danych lub przeniesienie wszystkich danych eksportowalnych i aktywów cyfrowych do lokalnej infrastruktury ICT bez zbędnej zwłoki i w żadnym razie nie później niż po upływie obowiązkowego maksymalnego okresu przejściowego wynoszącego 30 dni kalendarzowych i rozpoczynającego się po maksymalnym okresie wypowiedzenia, o którym mowa w lit. d), kiedy to umowa o świadczenie usług nadal ma zastosowanie, a dostawca usług przetwarzania danych:

      (i) zapewnia klientowi i osobom trzecim upoważnionym przez klienta uzasadnioną pomoc w procesie zmiany dostawcy;

(ii) postępuje z należytą starannością w celu utrzymania ciągłości działalności i kontynuuje świadczenie funkcji lub usług przewidzianych w umowie;

(iii) przedstawia jasne informacje o znanych zagrożeniach dla ciągłości świadczenia funkcji lub usług po stronie wyjściowego dostawcy usług przetwarzania danych;

(iv) zapewnia, aby w trakcie całego procesu zmiany dostawcy utrzymany został wysoki poziom bezpieczeństwa, w szczególności bezpieczeństwa danych podczas ich przekazywania i dalszego bezpieczeństwa danych podczas okresu zatrzymywania, o którym mowa w lit. c), zgodnie z mającymi zastosowanie przepisami prawa Unii lub prawa krajowego;

b) zobowiązanie dostawcy usług przetwarzania danych do wsparcia strategii odejścia klienta w odniesieniu do usług objętych umową, w tym poprzez przekazanie wszelkich istotnych informacji;

c) postanowienie umowne określające, że umowa zostaje uznana za rozwiązaną, a klient zostaje poinformowany o jej rozwiązaniu w jednym z następujących przypadków:

(i) w stosownym przypadku po pomyślnym zakończeniu procesu zmiany dostawcy;

(ii) na zakończenie maksymalnego okresu wypowiedzenia, o którym mowa w lit. d), w przypadku gdy klient nie chce zmienić dostawcy, ale chce usunąć wszystkie swoje dane eksportowalne i aktywa cyfrowe po zakończeniu usługi;

d) maksymalny okres wypowiedzenia rozpoczynający proces zmiany dostawcy i nieprzekraczający dwóch miesięcy;

e) szczegółowa specyfikacja wszystkich kategorii danych i aktywów cyfrowych, które można przenieść w trakcie procesu zmiany dostawcy, w tym co najmniej wszystkich danych eksportowalnych;

f) szczegółowa specyfikacja kategorii danych specyficznych dla wewnętrznego funkcjonowania dostawcy usługi przetwarzania danych, które są wyłączone spośród danych eksportowalnych przewidzianych w lit. e) niniejszego ustępu, w przypadku gdy istnieje ryzyko naruszenia tajemnic przedsiębiorstwa dostawcy, o ile wyłączenia te nie utrudniają ani nie opóźniają procesu zmiany dostawcy, o którym mowa w art. 23;

g) minimalny okres, w którym można pobrać dane, wynoszący co najmniej 30 dni kalendarzowych, rozpoczynający się po zakończeniu okresu przejściowego uzgodnionego między klientem a dostawcą usług przetwarzania danych, zgodnie z lit. a) niniejszego ustępu i ust. 4;

h) postanowienie umowne gwarantujące całkowite usunięcie wszystkich danych eksportowalnych i aktywów cyfrowych wygenerowanych bezpośrednio przez klienta lub bezpośrednio dotyczących klienta po upływie okresu pobierania, o którym mowa w lit. g), lub po upływie alternatywnego uzgodnionego okresu w terminie późniejszym niż termin upływu okresu pobierania, o którym mowa w lit. g), pod warunkiem że pomyślnie ukończony został proces zmiany dostawcy;

i) opłaty z tytułu zmiany dostawcy, które dostawcy usług przetwarzania danych mogą nałożyć zgodnie z art. 29.

3. Umowa, o której mowa w ust. 1, zawiera postanowienia umowne określające, że klient może powiadomić dostawcę usług przetwarzania danych o swojej decyzji, aby po upływie maksymalnego okresu wypowiedzenia, o którym mowa w ust. 2 lit. d), wykonać co najmniej jedno z następujących działań:

   a) zmienić dostawcę usług przetwarzania danych na innego dostawcę, w którym to przypadku klient przedstawia niezbędne dane tego innego dostawcy;

   b) przejść na lokalną infrastrukturę ICT;

   c) usunąć jego dane eksportowalne i aktywa cyfrowe.

4. W przypadku gdy obowiązkowy maksymalny okres przejściowy określony w ust. 2 lit. a) jest technicznie niemożliwy, dostawca usług przetwarzania danych powiadamia o tym klienta w terminie 14 dni roboczych od złożenia wniosku o zmianę dostawcy, należycie uzasadnia techniczną niewykonalność i wskazuje zastępczy okres przejściowy, który nie może przekroczyć siedmiu miesięcy. Zgodnie z ust. 1 ciągłość usługi zostaje zapewniona przez cały zastępczy okres przejściowy.

5. Bez uszczerbku dla ust. 4 umowa, o której mowa w ust. 1 zawiera postanowienia umowne zapewniające klientowi prawo do jednokrotnego przedłużenia okresu przejściowego o okres, który klient uznaje za właściwszy z uwagi na własne cele.

Artykuł 26

Obowiązek informacyjny spoczywający na dostawcach usług przetwarzania danych

Dostawca usług przetwarzania danych przedstawia klientowi:

a) informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych;

b) odniesienie do aktualnego rejestru internetowego prowadzonego przez dostawcę usług przetwarzania danych ze szczegółowymi informacjami o wszelkich strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne, o których mowa w art. 25 ust. 2 lit. e).

Artykuł 27

Obowiązek działania w dobrej wierze

Wszystkie zaangażowane strony, w tym docelowi dostawcy usług przetwarzania danych, współpracują ze sobą w dobrej wierze, aby zapewnić skuteczność procesu zmiany dostawcy, umożliwić terminowe przekazanie danych oraz utrzymać ciągłość usługi przetwarzania danych.

Artykuł 28

Umowne obowiązki dotyczące przejrzystości w zakresie dostępu międzynarodowego i przekazywania międzynarodowego

1. Dostawcy usług przetwarzania danych udostępniają na swoich stronach internetowych i na bieżąco aktualizują następujące informacje:

   a) jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług;

   b) ogólny opis środków technicznych, organizacyjnych i umownych przyjętych przez dostawcę usług przetwarzania danych w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

2. Odniesienie do stron internetowych, o których mowa w ust. 1, znajduje się w umowach w odniesieniu do wszystkich usług przetwarzania danych oferowanych przez dostawców usług przetwarzania danych.

Artykuł 29

Stopniowe wycofywanie opłat z tytułu zmiany dostawcy

1. Od dnia... [trzy lata od dnia wejścia w życie niniejszego rozporządzenia] r. dostawcy usług przetwarzania danych nie nakładają na klienta opłat z tytułu zmiany dostawcy za procedurę zmiany dostawcy.

2. Od dnia… [data wejścia w życie niniejszego rozporządzenia] r. do dnia... [trzy lata od dnia wejścia w życie niniejszego rozporządzenia] r. dostawcy usług przetwarzania danych mogą nakładać na klienta obniżone opłaty z tytułu zmiany dostawcy za procedurę zmiany dostawcy.

3. Obniżone opłaty z tytułu zmiany dostawcy, o których mowa w ust. 2, nie przekraczają kosztów poniesionych przez dostawcę usług przetwarzania danych i bezpośrednio związanych z danym procesem zmiany dostawcy.

4. Przed zawarciem umowy z klientem dostawca usług przetwarzania danych przedstawia przyszłemu klientowi jasne informacje o standardowych opłatach za usługę i karach za wcześniejsze rozwiązanie umowy, które mogą zostać nałożone, oraz o obniżonych opłatach z tytułu zmiany dostawcy, które mogą zostać nałożone w okresie, o którym mowa w ust. 2.

5. W stosownym przypadku dostawcy usług przetwarzania danych przedstawiają klientowi informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

6. W stosownym przypadku dostawcy usług przetwarzania danych publicznie przedstawiają informacje, o których mowa w ust. 4 i 5, klientom za pomocą specjalnej sekcji na swojej stronie internetowej lub w inny łatwo dostępny sposób.

7. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 45 służących uzupełnieniu niniejszego rozporządzenia poprzez wprowadzenie mechanizmu monitorowania, który pozwoli jej monitorować opłaty z tytułu zmiany dostawcy nakładane na rynku przez dostawców usług przetwarzania danych i tym samym zapewnić, aby wycofanie i obniżenie opłat z tytułu zmiany dostawcy zgodnie z ust. 1 i 2 niniejszego artykułu odbyło się w terminach określonych w tych ustępach.

Artykuł 30

Techniczne aspekty zmiany dostawcy

1. Dostawcy usług przetwarzania danych, które to usługi dotyczą skalowalnych i elastycznych zasobów obliczeniowych ograniczonych do elementów infrastruktury, takich jak serwery, sieci i zasoby wirtualne niezbędne do obsługi infrastruktury, ale nie zapewniają dostępu do usług operacyjnych, oprogramowania i aplikacji, które są przechowywane, w inny sposób przetwarzane lub wdrażane na tych elementach infrastruktury, zgodnie z art. 27 stosują wszelkie uzasadnione środki pozostające w ich mocy, aby ułatwić klientowi – po zmianie dostawcy na dostawcę usługi obejmującej usługę tego samego typu – osiągnięcie równoważności funkcjonalnej w ramach korzystania z docelowej usługi przetwarzania danych. Wyjściowy dostawca usług przetwarzania danych ułatwia proces zmiany dostawcy, zapewniając zasoby, odpowiednie informacje, dokumentację, wsparcie techniczne oraz w stosownym przypadku niezbędne narzędzia.

2. Dostawcy usług przetwarzania danych inni niż dostawcy, o których mowa w ust. 1, aby ułatwić zmianę dostawcy, nieodpłatnie udostępniają otwarte interfejsy w równym zakresie wszystkim swoim klientom i zainteresowanym docelowym dostawcom usług przetwarzania danych. Interfejsy te zawierają wystarczająco dużo informacji o danej usłudze, aby można było opracować oprogramowanie do komunikacji z tymi usługami do celów przenoszenia i interoperacyjności danych.

3. W przypadku usług przetwarzania danych innych niż usługi, o których mowa w ust. 1 niniejszego artykułu, dostawcy usług przetwarzania danych zapewniają zgodność ze wspólnymi specyfikacjami opartymi na otwartych specyfikacjach w zakresie interoperacyjności lub zharmonizowanych normach w zakresie interoperacyjności co najmniej 12 miesięcy po tym, jak odniesienia do tych wspólnych specyfikacji lub do norm zharmonizowanych w zakresie interoperacyjności usług przetwarzania danych zostaną opublikowane w centralnym repozytorium norm Unii dotyczących interoperacyjności usług przetwarzania danych, po publikacji w *Dzienniku Urzędowym Unii Europejskiej* aktów wykonawczych będących ich podstawą zgodnie z art. 35 ust. 7.

4. Dostawcy usług przetwarzania danych inni niż dostawcy, o których mowa w ust. 1 niniejszego artykułu, uaktualniają rejestr internetowy, o którym mowa w art. 26 lit. b), zgodnie ze swoimi obowiązkami przewidzianymi w ust. 3 niniejszego artykułu.

5. W przypadku zmiany dostawcy na dostawcę usługi tego samego typu, dla której wspólne specyfikacje lub normy zharmonizowane w zakresie interoperacyjności, o których mowa w ust. 3 niniejszego artykułu, nie zostały opublikowane się w centralnym repozytorium Unii dotyczącym interoperacyjności usług przetwarzania danych zgodnie z art. 35 ust. 8, dostawca usług przetwarzania danych na wniosek klienta eksportuje wszystkie dane eksportowalne w uporządkowanym, powszechnie używanym, nadającym się do odczytu maszynowego formacie.

6. Od dostawców usług przetwarzania danych nie wymaga się opracowania nowych technologii lub usług, ujawnienia lub przekazania zasobów cyfrowych chronionych prawami własności intelektualnej lub stanowiących tajemnicę przedsiębiorstwa klientowi lub innemu dostawcy usług przetwarzania danych ani stwarzania zagrożenia dla bezpieczeństwa i integralności usług klienta lub dostawcy.

Artykuł 31

Szczegółowe uregulowania dotyczące niektórych usług przetwarzania danych

1. Obowiązki określone w art. 23 lit. d), art. 29 i art. 30 ust. 1 i 3 nie mają zastosowania do usług przetwarzania danych, w przypadku których większość głównych cech została opracowana na zamówienie, tak aby dostosować je do konkretnych potrzeb indywidualnego klienta, lub w przypadku których wszystkie komponenty zostały opracowane na potrzeby indywidualnego klienta i w przypadku gdy te usługi przetwarzania danych nie są oferowane komercyjnie na szeroką skalę poprzez katalog usług dostawcy usług przetwarzania danych.

2. Obowiązki określone w niniejszym rozdziale nie mają zastosowania do usług przetwarzania danych świadczonych przez ograniczony okres jako nieprzeznaczona do produkcji wersja do celów testowania i oceny.

3. Przed zawarciem umowy o świadczenie usług przetwarzania danych, o których to usługach mowa w niniejszym artykule, dostawca usług przetwarzania danych informuje przyszłego klienta o obowiązkach przewidzianych w niniejszym rozdziale, które nie mają zastosowania.

Rozdział VII

Bezprawny międzynarodowy dostęp administracji rządowej do danych nieosobowych i bezprawne międzynarodowe przekazywanie danych nieosobowych

Artykuł 32

Międzynarodowy dostęp administracji rządowej i przekazywanie

1. Dostawcy usług przetwarzania danych stosują wszelkie odpowiednie środki techniczne, organizacyjne i prawne, w tym umowy, w celu zapobiegania międzynarodowemu dostępowi administracji rządowej państw trzecich do danych nieosobowych przechowywanych na terenie Unii oraz międzynarodowemu przekazywaniu takich danych nieosobowych, w przypadku gdy takie przekazywanie lub taki dostęp byłyby sprzeczne z prawem Unii lub prawem krajowym danego państwa członkowskiego, bez uszczerbku dla ust. 2 lub 3.

2. Orzeczenia lub wyroki sądu lub trybunału państwa trzeciego oraz decyzje organu administracyjnego państwa trzeciego nakazujące dostawcy usług przetwarzania danych przekazanie przechowywanych na terenie Unii danych nieosobowych objętych zakresem stosowania niniejszego rozporządzenia lub udzielenie dostępu do tych danych uznaje się lub wykonuje wyłącznie wtedy, gdy są oparte na umowie międzynarodowej, takiej jak traktat o pomocy prawnej, obowiązującej między państwem trzecim, które występuje z wnioskiem, a Unią lub na umowie tego rodzaju między państwem trzecim, które występuje z wnioskiem, a państwem członkowskim.

3. W przypadku braku umowy międzynarodowej, o której mowa w ust. 2, jeżeli dostawca usług przetwarzania danych jest adresatem orzeczenia lub wyroku sądu lub trybunału państwa trzeciego lub decyzji organu administracyjnego państwa trzeciego nakazujących przekazanie przechowywanych na terenie Unii danych nieosobowych objętych zakresem stosowania niniejszego rozporządzenia lub udzielenie dostępu do tych danych, a zastosowanie się do takiego orzeczenia lub takiej decyzji wiązałoby się z ryzykiem naruszenia przez adresata prawa Unii lub prawa krajowego stosownego państwa członkowskiego, przekazanie takich danych temu organowi państwa trzeciego lub udzielenie mu dostępu do takich danych odbywa się wyłącznie gdy:

   a) system państwa trzeciego wymaga, aby uzasadnienie i proporcjonalność takiego orzeczenia, wyroku lub takiej decyzji zostały określone oraz aby takie orzeczenie, wyrok lub taka decyzja miały konkretny charakter, np. poprzez ustalenie wystarczającego związku z niektórymi osobami podejrzanymi lub naruszeniami;

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

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

Adresat decyzji lub orzeczenia może zwrócić się o opinię do stosownego podmiotu lub organu krajowego właściwego ds. współpracy międzynarodowej w kwestiach prawnych w celu ustalenia, czy warunki określone w akapicie pierwszym zostały spełnione, w szczególności jeżeli uzna, że orzeczenie lub decyzja mogą dotyczyć tajemnic przedsiębiorstwa i innych szczególnie chronionych danych handlowych oraz treści chronionych prawami własności intelektualnej lub przekazanie może prowadzić do deanonimizacji. Właściwy podmiot lub organ krajowy może skonsultować się z Komisją. Jeżeli adresat uzna, że decyzja może naruszać bezpieczeństwo narodowe lub interesy obronne Unii lub jej państw członkowskich, zwraca się o opinię do właściwych podmiotów lub organów krajowych w celu ustalenia, czy żądane dane dotyczą bezpieczeństwa narodowego lub interesów obronnych Unii lub jej państw członkowskich. Jeżeli adresat nie otrzyma odpowiedzi w terminie miesiąca lub jeżeli właściwy podmiot lub organ krajowy stwierdzi w opinii, że warunki określone w akapicie pierwszym nie zostały spełnione, adresat może na tej podstawie odrzucić wniosek o przekazanie danych nieosobowych lub dostęp do nich.

Europejska Rada ds. Innowacji w zakresie Danych, o której mowa w art. 42, doradza Komisji i wspiera ją w opracowywaniu wytycznych w sprawie oceny spełnienia warunków określonych w akapicie pierwszym niniejszego ustępu.

4. Jeżeli spełnione są warunki określone w ust. 2 lub 3, dostawca usług przetwarzania danych w odpowiedzi na wniosek dostarcza jak najmniejszą ilość danych dozwoloną w oparciu o racjonalną interpretację tego wniosku dokonaną przez dostawcę lub właściwy krajowy podmiot lub organ, o którym mowa w ust. 3 akapit drugi.

5. Zanim dostawca usług przetwarzania danych zastosuje się do tego wniosku, informuje on klienta o wniosku organu państwa trzeciego o dostęp do jego danych, z wyjątkiem przypadków, w których wniosek służy do celów ścigania przestępstw i tak długo, jak jest to niezbędne do zachowania skuteczności działań w tym zakresie.

Rozdział VIII
Interoperacyjność

Artykuł 33

Zasadnicze wymagania w zakresie interoperacyjności danych, mechanizmów i usług dzielenia się danymi oraz wspólnych europejskich przestrzeni danych

1. Uczestnicy przestrzeni danych oferujący innym uczestnikom dane lub usługi oparte na danych spełniają następujące zasadnicze wymagania w celu ułatwienia interoperacyjności danych, mechanizmów i usług dzielenia się danymi oraz wspólnych europejskich przestrzeni danych, które są interoperacyjnymi ramami wspólnych norm i praktyk, szczególnymi dla danego celu lub sektora bądź międzysektorowymi, służącymi dzieleniu się danymi lub ich wspólnemu przetwarzaniu na potrzeby m.in. opracowywania nowych produktów i usług, badań naukowych lub inicjatyw społeczeństwa obywatelskiego:

   a) dostatecznie opisane są zawartość zestawu danych, ograniczenia wykorzystania, licencje, metody zbierania danych, jakość danych i niepewność, w stosownym przypadku w formacie nadającym się do odczytu maszynowego, aby umożliwić odbiorcy znalezienie danych, dostęp do nich i ich wykorzystanie;

   b) w ogólnodostępny i spójny sposób opisane są struktury danych, formaty danych, słowniki, systemy klasyfikacji, taksonomie i wykazy kodów, jeżeli są dostępne;

c) dostatecznie opisane są techniczne środki dostępu do danych, takie jak interfejsy programowania aplikacji, oraz warunki korzystania z tych środków i jakość usługi, aby umożliwić automatyczny dostęp do danych i ich przesyłanie między stronami, w tym w sposób ciągły, w sposób masowy lub w czasie rzeczywistym w formacie nadającym się do odczytu maszynowego, jeżeli jest to techniczne możliwe i nie utrudnia prawidłowego funkcjonowania produktu skomunikowanego;

d) w stosownym przypadku zapewnione są środki umożliwiające interoperacyjność narzędzi automatycznego wykonywania umów w sprawie dzielenia się danymi, takich jak inteligentne umowy.

Wymagania te mogą mieć charakter ogólny lub dotyczyć konkretnych sektorów, przy czym należy w pełni uwzględnić ich wzajemne powiązania z wymaganiami wynikającymi z prawa Unii lub z prawa krajowego.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 45 niniejszego rozporządzenia, w celu uzupełnienia niniejszego rozporządzenia poprzez doprecyzowanie zasadniczych wymagań określonych w ust. 1 niniejszego artykułu, w odniesieniu do tych wymagań, które ze względu na swój charakter nie mogą przynieść zamierzonego efektu, chyba że zostaną doprecyzowane w wiążących aktach prawnych Unii, i w celu właściwego odzwierciedlenia zmian technologicznych i rynkowych.

Przyjmując te akty delegowane, Komisja uwzględnia opinię Europejskiej Rady ds. Innowacji w zakresie Danych zgodnie z art. 42 lit. c) ppkt (iii).

3. Domniemywa się, że uczestnicy przestrzeni danych oferujący dane lub usługi oparte na danych innym uczestnikom przestrzeni danych i spełniający normy zharmonizowane lub części tych norm, do których odniesienia są opublikowane w *Dzienniku Urzędowym Unii Europejskiej*, spełniają zasadnicze wymagania, o których mowa w ust. 1, w zakresie, w jakim wspomniane wymagania objęte są takimi normami zharmonizowanymi lub ich częściami.

4. Komisja, zgodnie z art. 10 rozporządzenia (UE) nr 1025/2012, zwraca się do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o przygotowanie norm zharmonizowanych spełniających zasadnicze wymagania określone w ust. 1 niniejszego artykułu.

5. Komisja może przyjąć – w drodze aktów wykonawczych – wspólne specyfikacje, obejmujące dowolny lub wszystkie zasadnicze wymagania określone w ust. 1, jeżeli spełnione zostały następujące warunki:

   a) Komisja zwróciła się, zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012, do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o przygotowanie normy zharmonizowanej spełniającej zasadnicze wymagania określone w ust. 1 niniejszego artykułu, a w dodatku:

      (i) wniosek nie został zaakceptowany;

      (ii) normy zharmonizowane dotyczące tego wniosku nie zostały dostarczone w terminie określonym zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012; lub

      (iii) normy zharmonizowane nie są zgodne z wnioskiem; oraz

b) w *Dzienniku Urzędowym Unii Europejskiej* nie jest opublikowane odniesienie do norm zharmonizowanych obejmujących stosowne zasadnicze wymagania określone w ust. 1 niniejszego artykułu zgodnie z rozporządzeniem (UE) nr 1025/2012 i nie przewiduje się publikacji takiego odniesienia w rozsądnym terminie.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 46 ust. 2.

6. Przed sporządzeniem projektu aktu wykonawczego, o którym mowa w ust. 5 niniejszego artykułu Komisja informuje komitet, o którym mowa w art. 22 rozporządzenia (UE) nr 1025/2012, że jej zdaniem spełnione zostały warunki przewidziane w ust. 5 niniejszego artykułu.

7. Sporządzając projekt aktu wykonawczego, o którym mowa w ust. 5, Komisja uwzględnia opinie Europejskiej Rady ds. Innowacji w zakresie Danych i innych stosownych podmiotów lub grup ekspertów i należycie konsultuje się ze wszystkimi stosownymi zainteresowanymi stronami.

8. Domniemywa się, że uczestnicy przestrzeni danych oferujący dane lub usługi oparte na danych innym uczestnikom przestrzeni danych i spełniający wspólne specyfikacje ustanowione aktami wykonawczymi, o których mowa w ust. 5, lub ich części spełniają zasadnicze wymagania określone w ust. 1 objęte tymi wspólnymi specyfikacjami lub ich częściami.

9. W przypadku gdy norma zharmonizowana zostaje przyjęta przez europejską organizację normalizacyjną i przedstawiona Komisji w celu opublikowania odniesienia do niej w *Dzienniku Urzędowym Unii Europejskiej*, Komisja ocenia tę normę zharmonizowaną zgodnie z rozporządzeniem (UE) 1025/2012. W przypadku opublikowania odniesienia do normy zharmonizowanej w *Dzienniku Urzędowym Unii Europejskiej* Komisja uchyla akty wykonawcze, o których mowa w ust. 5 niniejszego artykułu, lub ich części, które obejmują te same zasadnicze wymagania, jak te objęte normą zharmonizowaną.

10. W przypadku gdy państwo członkowskie uzna, że wspólna specyfikacja nie w pełni spełnia zasadnicze wymagania określone w ust. 1, informuje o tym Komisję, przedstawiając szczegółowe wyjaśnienie. Komisja ocenia to szczegółowe wyjaśnienie i w stosownym przypadku może zmienić akt wykonawczy ustanawiający daną wspólną specyfikację.

11. Komisja może przyjąć wytyczne, uwzględniając propozycję Europejskiej Rady ds. Innowacji w zakresie Danych zgodnie z art. 30 lit. h) rozporządzenia (UE) 868/2022, ustanawiającym specyfikacje w zakresie interoperacyjnych ram wspólnych norm i praktyk na potrzeby funkcjonowania wspólnych europejskich przestrzeni danych.

Artykuł 34

Interoperacyjność do celów równoczesnego korzystania z usług przetwarzania danych

1. Wymagania określone w art. 23, 24, 25 ust. 2 lit. a) pkt (ii) i (iv), lit. e) i f) oraz w art. 30 ust. 2 do 5 mają także zastosowanie odpowiednio do dostawców usług przetwarzania danych, aby ułatwić interoperacyjność do celów równoczesnego korzystania z usług przetwarzania danych.

2. W przypadku równoczesnego korzystania z usług przetwarzania danych, dostawcy usług przetwarzania danych mogą nałożyć opłaty z tytułu wychodzącego ruchu, które nie przekraczają poniesionych kosztów z tytułu wychodzącego ruchu.

Artykuł 35

Interoperacyjność usług przetwarzania danych

1. Otwarte specyfikacje w zakresie interoperacyjności i normy zharmonizowane w zakresie interoperacyjności usług przetwarzania danych:

   a) zapewniają, jeżeli jest to technicznie możliwe, interoperacyjność różnych usług przetwarzania danych, które obejmują usługi tego samego typu;

   b) zwiększają możliwość przenoszenia aktywów cyfrowych między różnymi usługami przetwarzania danych, które obejmują usługi tego samego typu;

   c) ułatwiają, jeżeli jest to technicznie możliwe, równoważność funkcjonalną różnych usług przetwarzania danych określonych w art. 30 ust. 1, które obejmują usługi tego samego typu;

d) nie wpływają negatywnie na bezpieczeństwo i integralność usług przetwarzania danych i danych;

e) są opracowywane w sposób umożliwiający postęp techniczny oraz wprowadzanie nowych funkcji i innowacji w usługach przetwarzania danych.

2. Otwarte specyfikacje w zakresie interoperacyjności i normy zharmonizowane w zakresie interoperacyjności usług przetwarzania danych odpowiednio dotyczą:

a) aspektów interoperacyjności w chmurze w odniesieniu do interoperacyjności przesyłu danych, interoperacyjności syntaktycznej, interoperacyjności semantycznej danych, interoperacyjności behawioralnej i interoperacyjności zasad;

b) aspektów możliwości przenoszenia danych w chmurze w odniesieniu do syntaktycznej możliwości przenoszenia danych, semantycznej możliwości przenoszenia danych i możliwości przenoszenia zasad dotyczących danych;

c) aspektów aplikacji w chmurze w odniesieniu do syntaktycznej możliwości przenoszenia aplikacji, możliwości przenoszenia poleceń aplikacji, możliwości przenoszenia metadanych aplikacji, możliwości przenoszenia zachowania aplikacji i możliwości przenoszenia zasad aplikacji.

3. Otwarte specyfikacje w zakresie interoperacyjności są zgodne z załącznikiem II do rozporządzenia (UE) nr 1025/2012.

4. Po uwzględnieniu stosownych międzynarodowych i europejskich norm i inicjatyw samoregulacyjnych Komisja może, zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012, zwrócić się do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o przygotowanie norm zharmonizowanych spełniających zasadnicze wymagania określone w ust. 1 i 2 niniejszego artykułu.

5. Komisja może przyjąć – w drodze aktów wykonawczych – wspólne specyfikacje na podstawie otwartych specyfikacji w zakresie interoperacyjności, obejmujące wszystkie zasadnicze wymagania określone w ust. 1 i 2.

6. Sporządzając projekt aktu wykonawczego, o którym mowa w u ust. 5 niniejszego artykułu, Komisja uwzględnia opinię właściwych organów krajowych, o których mowa w art. 37 ust. 5 lit. h), oraz innych właściwych podmiotów lub grup ekspertów i należycie konsultuje się ze wszystkimi właściwymi zainteresowanymi stronami.

7. W przypadku gdy państwo członkowskie uzna, że wspólna specyfikacja nie w pełni spełnia zasadnicze wymagania określone w ust. 1 i 2, informuje o tym Komisję, przedstawiając szczegółowe wyjaśnienie. Komisja ocenia to szczegółowe wyjaśnienie i w stosownym przypadku może zmienić akt wykonawczy ustanawiający daną wspólną specyfikację.

8. Do celów art. 30 ust. 3 Komisja publikuje – w drodze aktów wykonawczych – odniesienia do norm zharmonizowanych i wspólnych specyfikacji w zakresie interoperacyjności usług przetwarzania danych w centralnym unijnym repozytorium norm dotyczących interoperacyjności usług przetwarzania danych.

9. Akty wykonawcze, o których mowa w niniejszym artykule, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 46 ust. 2.

Artykuł 36

Zasadnicze wymagania dotyczące inteligentnych umów na potrzeby wykonywania umów w sprawie dzielenia się danymi

1. Dostawca aplikacji wykorzystującej inteligentne umowy lub w przypadku jego braku osoba, której działalność handlowa, gospodarcza lub zawodowa obejmuje wdrażanie inteligentnych umów dla innych osób w kontekście wykonywania umowy o udostępnianie danych lub jej części zapewnia, aby inteligentne umowy spełniały następujące zasadnicze wymagania:

   a) odporność i kontrola dostępu, zapewniające, aby inteligentna umowa została opracowana w sposób umożliwiający mechanizmy kontroli dostępu i bardzo wysoki poziom odporności na błędy funkcjonalne i manipulacje ze strony osób trzecich;

   b) bezpieczne zakończenie i przerwanie, zapewniające, aby istniał mechanizm umożliwiający zakończenie dalszej realizacji transakcji oraz, aby inteligentna umowa obejmowała funkcje wewnętrzne, które mogą zresetować umowę lub polecić umowie zakończenie lub przerwanie działania, w szczególności w celu uniknięcia przyszłego przypadkowego wykonania;

   c) archiwizacja i ciągłość danych, zapewniające, aby w warunkach, w których inteligentna umowa musi zostać zakończona lub dezaktywowana, istniała możliwość archiwizacji danych transakcyjnych oraz logiki i kodu inteligentnej umowy w celu zachowania rejestru operacji wykonanych na danych w przeszłości (możliwość kontroli);

d) kontrola dostępu, zapewniająca, aby inteligentna umowa była chroniona za pomocą rygorystycznych mechanizmów kontroli dostępu w warstwach zarządzania i inteligentnych umów; oraz

e) spójność, zapewniająca spójność z postanowieniami umowy o dzieleniu się danymi, którą inteligentna umowa wykonuje.

2. Dostawca inteligentnej umowy lub w przypadku jego braku osoba, której działalność handlowa, gospodarcza lub zawodowa obejmuje wdrażanie inteligentnych umów dla innych osób w kontekście wykonywania umowy lub jej części w sprawie udostępniania danych, przeprowadza ocenę zgodności w celu spełnienia zasadniczych wymagań określonych w ust. 1 i wydaje deklarację zgodności UE, jeżeli wymagania te są spełnione.

3. Sporządzając deklarację zgodności UE, dostawca aplikacji wykorzystującej inteligentne umowy lub w przypadku jego braku osoba, której działalność handlowa, gospodarcza lub zawodowa obejmuje wdrażanie inteligentnych umów dla innych osób w kontekście wykonania umowy, lub jej części, w sprawie udostępniania danych, są odpowiedzialni za przestrzeganie wymagań określonych w ust. 1.

4. Domniemywa się, że inteligentna umowa, która spełnia normy zharmonizowane lub stosowne części tych norm, do których odniesienia są opublikowane w *Dzienniku Urzędowym Unii Europejskiej*, jest zgodna z zasadniczymi wymaganiami określonymi w ust. 1 w zakresie, w jakim wymagania te są objęte takimi normami zharmonizowanymi lub ich częścią.

5. Komisja, zgodnie z art. 10 rozporządzenia (UE) nr 1025/2012, zwraca się do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o przygotowanie norm zharmonizowanych spełniających zasadnicze wymagania określone w ust. 1 niniejszego artykułu.

6. Komisja może przyjąć – w drodze aktów wykonawczych – wspólne specyfikacje, obejmujące dowolne lub wszystkie zasadnicze wymagania określone w ust. 1, jeżeli spełnione zostały następujące warunki:

   a) Komisja zwróciła się, zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012, do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o przygotowanie normy zharmonizowanej spełniającej zasadnicze wymagania określone w ust. 1 niniejszego artykułu, a w dodatku

      (i) wniosek nie został zaakceptowany;

      (ii) normy zharmonizowane dotyczące tego wniosku nie zostały dostarczone w terminie określonym zgodnie z art. 10 ust. 1 rozporządzenia (UE) nr 1025/2012; lub

      (iii) normy zharmonizowane nie są zgodne z wnioskiem; oraz

   b) w *Dzienniku Urzędowym Unii Europejskiej* nie jest opublikowane odniesienie do norm zharmonizowanych obejmujących stosowne zasadnicze wymagania określone w ust. 1 niniejszego artykułu zgodnie z rozporządzeniem (UE) nr 1025/2012 i nie przewiduje się publikacji takiego odniesienia w rozsądnym terminie.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 46 ust. 2.

7. Przed sporządzeniem projektu aktu wykonawczego, o którym mowa w ust. 6 niniejszego artykułu Komisja informuje komitet, o którym mowa w art. 22 rozporządzenia (UE) nr 1025/2012, że jej zdaniem spełnione zostały warunki przewidziane w ust. 6 niniejszego artykułu.

8. Sporządzając projekt aktu wykonawczego, o którym mowa w ust. 6, Komisja uwzględnia opinie Europejskiej Rady ds. Innowacji w zakresie Danych i innych stosownych podmiotów lub grup ekspertów i należycie konsultuje się ze wszystkimi stosownymi zainteresowanymi stronami.

9. Domniemywa się, że dostawca inteligentnej umowy lub w przypadku jego braku osoba, której działalność handlowa, gospodarcza lub zawodowa obejmuje wdrażanie inteligentnych umów dla innych osób w kontekście wykonywania umowy o udostępnianiu danych lub jej części, spełniający wspólne specyfikacje ustanowione aktami wykonawczymi, o których mowa w ust. 6, lub ich częściami, spełniają zasadnicze wymagania określone w ust. 1 w takim zakresie, że wymagania te objęte są takimi wspólnymi specyfikacjami lub ich częściami.

10. W przypadku gdy norma zharmonizowana zostaje przyjęta przez europejską organizację normalizacyjną i przedstawiona Komisji w celu opublikowania odniesienia do niej w *Dzienniku Urzędowym Unii Europejskiej*, Komisja ocenia normę zharmonizowaną zgodnie z rozporządzeniem (UE) 1025/2012. W przypadku publikacji odniesienia do normy zharmonizowanej w *Dzienniku Urzędowym Unii Europejskiej* Komisja uchyla akty wykonawcze, o których mowa w ust. 6 niniejszego artykułu, lub ich części, które obejmują te same zasadnicze wymagania, takie jak te objęte przez tę normę zharmonizowaną.

11. W przypadku gdy państwo członkowskie uzna, że wspólna specyfikacja niecałkowicie spełnia zasadnicze wymagania określone w ust. 1, informuje o tym Komisję, przedstawiając szczegółowe wyjaśnienie. Komisja ocenia to szczegółowe wyjaśnienie i w stosownym przypadku może zmienić akt wykonawczy ustanawiający daną wspólną specyfikację.

Rozdział IX
Wdrażanie i egzekwowanie

Artykuł 37

Właściwe organy i koordynatorzy danych

1. Każde państwo członkowskie wyznacza właściwy organ lub właściwe organy odpowiedzialne za stosowanie i egzekwowanie niniejszego rozporządzenia (zwane dalej „właściwymi organami”). Państwa członkowskie mogą ustanowić co najmniej jeden nowy organ lub oprzeć się na organach już istniejących.

2. W przypadku gdy państwo członkowskie wyznaczy więcej niż jeden właściwy organ, wyznacza spośród nich koordynatora danych, który ułatwia współpracę między właściwymi organami i pomaga podmiotom objętym zakresem stosowania niniejszego rozporządzenia we wszystkich sprawach związanych z jego stosowaniem i egzekwowaniem. Właściwe organy, wykonując zadania i uprawnienia przyznane im na podstawie ust. 5, współpracują ze sobą nawzajem.

3. Organy nadzorcze odpowiedzialne za monitorowanie stosowania rozporządzenia (UE) 2016/679 są odpowiedzialne za monitorowanie stosowania niniejszego rozporządzenia w zakresie ochrony danych osobowych. Stosuje się odpowiednio rozdziały VI i VII rozporządzenia (UE) 2016/679.

Europejski Inspektor Ochrony Danych jest odpowiedzialny za monitorowanie stosowania niniejszego rozporządzenia w zakresie, w jakim dotyczy ono Komisji, Europejskiego Banku Centralnego lub organów Unii. W stosownym przypadku stosuje się odpowiednio art. 62 rozporządzenia (UE) 2018/1725.

Zadania i uprawnienia organów nadzorczych, o których mowa w niniejszym ustępie, są wykonywane w odniesieniu do przetwarzania danych osobowych.

4. Bez uszczerbku dla ust. 1 niniejszego artykułu:

a) w odniesieniu do konkretnych kwestii sektorowych dotyczących dostępu do danych i wykorzystywania danych w związku ze stosowaniem niniejszego rozporządzenia respektuje się kompetencje organów sektorowych;

b) właściwy organ odpowiedzialny za stosowanie i egzekwowanie art. 23 do 31 oraz art. 34 i 35 posiada doświadczenie w dziedzinie usług opartych na danych i usług łączności elektronicznej.

5. Państwa członkowskie zapewniają, aby zadania i uprawnienia właściwych organów były jasno określone i obejmowały:

a) propagowanie wśród użytkowników i podmiotów objętych zakresem stosowania niniejszego rozporządzenia umiejętności korzystania z danych oraz wiedzy na temat praw i obowiązków wynikających z niniejszego rozporządzenia;

b) rozpatrywanie skarg wynikających z domniemanych naruszeń niniejszego rozporządzenia, w tym związanych z tajemnicami przedsiębiorstwa, oraz prowadzenie postępowań, w odpowiednim zakresie, w przedmiocie skarg i regularne informowanie skarżącego, w stosownym przypadku zgodnie z prawem krajowym, w rozsądnym terminie o postępach i wynikach postępowania, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowania lub koordynacja działań z innym właściwym organem;

c) prowadzenie postępowań w sprawach dotyczących stosowania niniejszego rozporządzenia, w tym na podstawie informacji otrzymanych od innego właściwego organu lub innego organu publicznego;

d) nakładanie skutecznych, proporcjonalnych i odstraszających kar pieniężnych, które mogą obejmować kary okresowe i kary z mocą wsteczną, lub wszczynanie postępowań sądowych w celu nałożenia grzywny;

e) monitorowanie rozwoju technologicznego i sytuacji gospodarczej mających znaczenie dla udostępniania i wykorzystywania danych;

f) współpracę z właściwymi organami innych państw członkowskich oraz w stosownym przypadku z Komisją lub Europejską Radą ds. Innowacji w zakresie Danych w celu zapewnienia spójnego i skutecznego stosowania niniejszego rozporządzenia, w tym wymianę wszystkich istotnych informacji drogą elektroniczną bez zbędnej zwłoki, w tym w odniesieniu do ust. 10 niniejszego artykułu.;

g) współpracę ze stosownymi właściwymi organami odpowiedzialnymi za wdrażanie innych unijnych lub krajowych aktów prawnych, w tym organami właściwymi do spraw usług opartych na danych i usług łączności elektronicznej, organem nadzorczym odpowiedzialnym za monitorowanie stosowania rozporządzenia (UE) 2016/679 lub z organami sektorowymi w celu zapewnienia, aby niniejsze rozporządzenie było egzekwowane spójnie z innym prawem Unii i prawem krajowym;

h) współpracę ze stosownymi właściwymi organami w celu zapewnienia, aby obowiązki określone w art. 23 do 31 oraz art. 34 i 35 były egzekwowane spójnie z innymi prawem Unii i samoregulacją mającymi zastosowanie do dostawców usług przetwarzania danych;

i) zapewnienie wycofania opłat z tytułu zmiany dostawcy zgodnie z art. 29;

j) analizę wniosków o dane złożonych na podstawie rozdziału V.

W przypadku gdy wyznaczony został koordynator danych, ułatwia on współpracę o której mowa w lit. f), g) i h) akapitu pierwszego i na żądanie wspiera właściwe organy.

6. Koordynator danych, w przypadku gdy taki właściwy organ został wyznaczony:

a) działa jako pojedynczy punkt kontaktu we wszystkich sprawach związanych ze stosowaniem niniejszego rozporządzenia;

b) zapewnia publiczną dostępność w internecie wniosków o udostępnienie danych składanych przez organy sektora publicznego w przypadku wyjątkowej potrzeby na podstawie przepisów rozdziału V i promuje dobrowolne umowy o dzieleniu się danymi między organami sektora publicznego a posiadaczami danych;

c) co roku informuje Komisję o odmowach, o których powiadomiono go na podstawie art. 4 ust. 2 i 8 i art. 5 ust. 11.

7. Państwa członkowskie przekazują Komisji nazwy właściwych organów oraz ich zadania i uprawnienia, a także w stosownym przypadku nazwę koordynatora danych. Komisja prowadzi publiczny rejestr tych organów.

8. Wykonując swoje zadania i uprawnienia zgodnie z niniejszym rozporządzeniem, właściwe organy pozostają bezstronne i wolne od jakichkolwiek bezpośrednich i pośrednich wpływów zewnętrznych ani nie zwracają się o instrukcje w indywidualnych sprawach do żadnego innego organu publicznego ani podmiotu prywatnego ani nie przyjmują takich instrukcji.

9. Państwa członkowskie zapewniają, aby właściwe organy dysponowały wystarczającymi zasobami ludzkimi i technicznymi oraz stosowną wiedzą ekspercką umożliwiającymi im skuteczne wykonywanie zadań zgodnie z niniejszym rozporządzeniem.

10. Podmioty objęte zakresem stosowania niniejszego rozporządzenia podlegają kompetencji państwa członkowskiego, w którym dany podmiot ma siedzibę. W przypadku gdy podmiot ma siedzibę w więcej niż jednym państwie członkowskim, uznaje się, że podlega kompetencji państwa członkowskiego, w którym ma główną siedzibę, to znaczy w którym mieści się jego siedziba zarządu lub siedziba statutowa, z których wykonywane są podstawowe funkcje finansowe i sprawowana jest kontrola operacyjna.

11. Podmiot objęty zakresem stosowania niniejszego rozporządzenia, który udostępnia produkty skomunikowane lub oferuje usługi w Unii i który nie ma siedziby w Unii, wyznacza przedstawiciela prawnego w jednym z państw członkowskich.

12. Do celów przestrzegania niniejszego rozporządzenia przedstawiciel prawny zostaje upoważniony przez podmiot objęty zakresem stosowania niniejszego rozporządzenia, który udostępnia produkty skomunikowane lub oferuje usługi w Unii, by oprócz tego podmiotu lub zamiast niego właściwe organy kontaktowały się z nim we wszystkich kwestiach związanych z tym podmiotem. Przedstawiciel prawny współpracuje z właściwymi organami i na żądanie szczegółowo przedstawia im działania podjęte i przepisy przyjęte w celu zapewnienia przestrzegania niniejszego rozporządzenia przez podmiot objęty zakresem stosowania niniejszego rozporządzenia, który udostępnia produkty skomunikowane lub oferuje usługi w Unii.

13. Uznaje się, że podmiot objęty zakresem stosowania niniejszego rozporządzenia, który udostępnia produkty skomunikowane lub oferuje usługi w Unii, podlega kompetencji państwa członkowskiego, w którym zlokalizowany jest przedstawiciel prawny. Wyznaczenie przedstawiciela prawnego przez taki podmiot pozostaje bez uszczerbku dla odpowiedzialności i wszelkich postępowań, które mogą zostać wszczęte przeciwko, takiego podmiotu. Do czasu aż podmiot wyznaczy przedstawiciela prawnego zgodnie z niniejszym artykułem, w stosownym przypadku podlega on kompetencji wszystkich państw członkowskich do celów zapewnienia stosowania i egzekwowania niniejszego rozporządzenia. Dowolny właściwy organ może wykonać swoją właściwość, w tym nakładając skuteczne, proporcjonalne i odstraszające kary, pod warunkiem że dany podmiot nie podlega postępowaniu w sprawie egzekucji niniejszego rozporządzenia w związku z tym samymi faktami przez inny właściwy organ.

14. Właściwe organy mogą żądać od użytkowników, posiadaczy danych, odbiorców danych lub ich przedstawicieli prawnych podlegających kompetencji ich państwa członkowskiego wszelkich informacji niezbędnych do zweryfikowania przestrzegania niniejszego rozporządzenia. Każdy wniosek o informacje musi być proporcjonalny do zadania będącego jego podstawą i musi być uzasadniony.

15. W przypadku gdy właściwy organ jednego państwa członkowskiego zwraca się o pomoc lub środki egzekucji do właściwego organu innego państwa członkowskiego, przedkłada uzasadniony wniosek. Właściwy organ po otrzymaniu takiego wniosku bez zbędnej zwłoki odpowiada, szczegółowo przedstawiając podjęte lub planowane działania.

16. Właściwe organy przestrzegają zasad poufności oraz tajemnic służbowych i handlowych oraz chronią dane osobowe zgodnie z prawem Unii lub prawem krajowym. Wszelkie informacje wymienione w ramach wniosku o pomoc i zapewnione zgodnie z niniejszym artykułem są wykorzystywane wyłącznie w odniesieniu do sprawy, w której o nie wystąpiono.

Artykuł 38

Prawo do wniesienia skargi

1. Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej osoby fizyczne i prawne mają prawo wnieść skargę, indywidualnie lub w stosownym przypadku zbiorowo, do stosownego właściwego organu w państwie członkowskim, w którym mają miejsce zwykłego pobytu, miejsce pracy lub siedzibę, jeżeli sądzą, że ich prawa wynikające z niniejszego rozporządzenia zostały naruszone. Koordynator danych na wniosek przedstawia osobom fizycznym i prawnym wszelkie informacje niezbędne do wniesienia skargi do odpowiedniego właściwego organu.

2. Właściwy organ, do którego wniesiono skargę, informuje skarżącego zgodnie z prawem krajowym o przebiegu postępowania i podjętej decyzji.

3. Właściwe organy współpracują w celu skutecznego i terminowego rozpatrywania i rozstrzygania skarg, w tym poprzez wymianę wszelkich istotnych informacji drogą elektroniczną, bez zbędnej zwłoki. Współpraca ta nie wpływa na mechanizmy współpracy przewidziane w rozdziałach VI i VII rozporządzenia (UE) 2016/679 i w rozporządzeniu (UE) 2017/2394.

Artykuł 39

Prawo do skutecznego sądowego środka ochrony prawnej

1. Niezależnie od administracyjnych lub innych pozasądowych środków ochrony prawnej każda osoba fizyczna i prawna, których to dotyczy, ma prawo do skutecznego sądowego środka ochrony prawnej przeciwko prawnie wiążącej decyzji właściwych organów.

2. W przypadku gdy właściwy organ nie podejmie działań w odpowiedzi na skargę, każda osoba fizyczna i prawna, których to dotyczy, ma zgodnie z prawem krajowym prawo do skutecznego sądowego środka ochrony prawnej albo do skorzystania z kontroli dokonywanej przez bezstronny organ dysponujący odpowiednią wiedzą specjalistyczną.

3. Postępowania na podstawie niniejszego artykułu toczą się przed sądami lub trybunałami państwa członkowskiego, w którym znajduje się właściwy organ, przeciwko któremu sądowy środek ochrony prawnej został wniesiony indywidualnie lub – w stosownym przypadku – zbiorowo przez przedstawicieli osoby fizycznej lub prawnej lub kilka takich osób.

Artykuł 40

Kary

1. Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane kary są skuteczne, proporcjonalne i odstraszające.

2. Do dnia... [20 miesięcy od dnia wejścia w życie niniejszego rozporządzenia] państwa członkowskie powiadamiają Komisję o tych przepisach i środkach i bezzwłocznie informują ją o wszelkich późniejszych zmianach mających na nie wpływ. Komisja prowadzi i regularnie aktualizuje łatwo dostępny publiczny rejestr tych środków.

3. Państwa członkowskie uwzględniają zalecenia Europejskiej Rady ds. Innowacji w zakresie Danych oraz następujące niewyczerpujące kryteria nakładania kar za naruszenia niniejszego rozporządzenia:

   a) charakter, waga, skala i czas trwania naruszenia;

   b) wszelkie działania podjęte przez stronę naruszającą w celu złagodzenia skutków lub naprawienia szkody spowodowanej naruszeniem;

   c) wszelkie wcześniejsze naruszenia dokonane przez stronę naruszającą;

   d) korzyści finansowe uzyskane lub straty uniknięte przez stronę naruszającą w wyniku naruszenia, o ile takie korzyści lub straty można wiarygodnie ustalić;

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

f) roczny obrót strony naruszającej w Unii w poprzednim roku budżetowym.

4. Za naruszenia obowiązków ustanowionych w rozdziałach II, III i V niniejszego rozporządzenia organy nadzorcze odpowiedzialne za monitorowanie stosowania rozporządzenia (UE) 2016/679, mogą w zakresie swoich kompetencji nakładać administracyjne kary pieniężne zgodnie z art. 83 rozporządzenia (UE) 2016/679 do wysokości, o której mowa w art. 83 ust. 5 tego rozporządzenia.

5. Za naruszenia obowiązków ustanowionych w rozdziale V niniejszego rozporządzenia Europejski Inspektor Ochrony Danych może w zakresie swoich kompetencji nakładać administracyjne kary pieniężne zgodnie z art. 66 rozporządzenia (UE) 2018/1725 do wysokości, o której mowa w art. 66 ust. 3 tego rozporządzenia.

Artykuł 41

Modelowe postanowienia umowne i standardowe postanowienia umowne

Przed dniem ... [20 miesięcy od dnia wejścia w życie niniejszego rozporządzenia] Komisja opracowuje i zaleca niewiążące modelowe postanowienia umowne dotyczące dostępu do danych i ich wykorzystywania, w tym postanowienia dotyczące zasadnej rekompensaty i ochrony tajemnic przedsiębiorstwa, oraz niewiążące standardowe postanowienia umowne na potrzeby umów o przetwarzanie w chmurze, aby pomóc stronom w sporządzaniu i negocjowaniu kontraktów przewidujących sprawiedliwe, zasadne i niedyskryminujące prawa i obowiązki umowne.

Artykuł 42

Rola Europejskiej Rady ds. Innowacji w zakresie Danych

Europejska Rada ds. Innowacji w zakresie Danych, ustanowiona przez Komisję jako grupa ekspertów zgodnie z art. 29 rozporządzenia (UE) 2022/868, w której reprezentowane są właściwe organy, wspiera spójne stosowanie niniejszego rozporządzenia poprzez:

a) doradzanie i pomoc Komisji w odniesieniu do stworzenia spójnej praktyki właściwych organów w egzekwowaniu rozdziałów II, III, V i VII;

b) ułatwianie współpracy między właściwymi organami poprzez budowę zdolności i wymianę informacji, w szczególności poprzez ustanowienie metod skutecznej wymiany informacji związanych z egzekwowaniem praw i obowiązków na podstawie rozdziałów II, III i V w sprawach transgranicznych, w tym koordynację dotyczącą ustalania kar;

c) doradzanie i pomoc Komisji w:

   (i) podjęciu decyzji, czy wystąpić z wnioskiem o przygotowanie norm zharmonizowanych, o których mowa w art. 33 ust. 4, art. 35 ust. 4 i art. 36 ust. 5;

   (ii) opracowaniu aktów wykonawczych, o których mowa w art. 33 ust. 5, art. 35 ust. 5 i 8 oraz art. 36 ust. 6;

   (iii) opracowaniu aktów delegowanych, o których mowa w art. 29 ust. 7 i art. 33 ust. 2; oraz

(iv) przyjęciu wytycznych ustanawiających specyfikacje w zakresie interoperacyjnych ram wspólnych norm i praktyk na potrzeby funkcjonowania wspólnych europejskich przestrzeni danych, o których mowa w art. 33 ust. 11.

Rozdział X

Prawo *sui generis* przewidziane w dyrektywie 96/9/WE

Artykuł 43

Bazy danych zawierające określone dane

Prawo *sui generis* przewidziane w art. 7 dyrektywy 96/9/WE nie ma zastosowania, w przypadku gdy dane są pozyskiwane lub generowane z produktu skomunikowanego lub usługi powiązanej objętych zakresem stosowania niniejszego rozporządzenia, w szczególności w związku z jego art. 4 i 5.

Rozdział XI

Przepisy końcowe

Artykuł 44

Inne akty prawne Unii regulujące prawa i obowiązki w zakresie dostępu do danych i ich wykorzystywania

1. Obowiązki szczególne w zakresie udostępniania danych między przedsiębiorcami, między przedsiębiorcami a konsumentami oraz w wyjątkowych przypadkach między przedsiębiorcami a organami publicznymi, określone w aktach prawnych Unii, które weszły w życie do dnia... [dzień wejścia w życie niniejszego rozporządzenia] r. włącznie, oraz w aktach delegowanych lub wykonawczych przyjętych na ich podstawie, pozostają bez zmian.

2. Niniejsze rozporządzenie pozostaje bez uszczerbku dla prawa Unii określającego w świetle potrzeb sektora, wspólnej europejskiej przestrzeni danych lub obszaru służącego interesowi publicznemu dalsze wymagania, w szczególności w odniesieniu do:

a) technicznych aspektów dostępu do danych;

b) ograniczeń praw posiadaczy danych do dostępu do określonych danych dostarczonych przez użytkowników lub wykorzystywania tych danych;

c) aspektów wykraczających poza dostęp do danych i ich wykorzystywanie.

3. Niniejsze rozporządzenie z wyjątkiem rozdziału V pozostaje bez uszczerbku dla prawa Unii i prawa krajowego przewidujących dostęp do danych do celów badań naukowych i upoważniających do ich wykorzystania.

Artykuł 45

Wykonywanie przekazanych uprawnień

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

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 29 ust. 7 i art. 33 ust. 2, powierza się Komisji na czas nieokreślony od dnia... [dzień wejścia w życie niniejszego rozporządzenia].

3. Przekazanie uprawnień, o którym mowa w art. 29 ust. 7 i art. 33 ust. 2, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

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

6. Akt delegowany przyjęty na podstawie art. 29 ust. 7 lub art. 33 ust. 2 wchodzi w życie wyłącznie wtedy, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 46

Procedura komitetowa

1. Komisję wspomaga komitet ustanowiony na mocy rozporządzenia (UE) 2022/868. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 47

Zmiana w rozporządzeniu (UE) 2017/2394

W załączniku do rozporządzenia (UE) 2017/2394 dodaje się punkt w brzmieniu:

„29. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/… z dnia... 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.U. L...)[+].”

Artykuł 48

Zmiana w dyrektywie (UE) 2020/1828

W załączniku I do dyrektywy (UE) 2020/1828 dodaje się punkt w brzmieniu:

„68. Rozporządzenie Parlamentu Europejskiego i Rady (UE) XXX z dnia... 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.U. L...)[+].”.

[+] Dz.U.: proszę wstawić w tekście numer rozporządzenia zamieszczonego w dokumencie PE CONS 49/23 (2022/0047(COD)), jego datę oraz odniesienie do Dz.U.

Artykuł 49

Ocena i przegląd

1. Do dnia... [56 miesięcy od dnia wejścia w życie niniejszego rozporządzenia] Komisja przeprowadza ocenę niniejszego rozporządzenia i przedkłada Parlamentowi Europejskiemu i Radzie, a także Europejskiemu Komitetowi Ekonomiczno-Społecznemu sprawozdanie na temat głównych ustaleń. Ocena ta obejmuje w szczególności:

   a) sytuacje uznawane za sytuacje wyjątkowej potrzeby do celów art. 15 niniejszego rozporządzenia i stosowanie rozdziału V niniejszego rozporządzenia w praktyce, w szczególności doświadczenie organów sektora publicznego, Komisji, Europejskiego Banku Centralnego oraz organów Unii w stosowaniu rozdziału V niniejszego rozporządzenia; liczbę i wynik postępowań wniesionych do właściwego organu na podstawie art. 18 ust. 5 w sprawie stosowania rozdziału V niniejszego rozporządzenia, zgodnie ze zgłoszeniami właściwych organów; skutki innych obowiązków ustanowionych w prawie Unii i prawie krajowym do celów realizacji wniosków o dostęp do informacji; wpływ mechanizmów dobrowolnego dzielenia się danymi, takich jak tych ustanowionych przez organizacje altruizmu danych uznane na podstawie rozporządzenia (UE) 2022/868, na realizację celów rozdziału V niniejszego rozporządzenia oraz rolę danych osobowych w kontekście art. 15 niniejszego rozporządzenia, w tym ewolucję technologii zwiększających prywatność;

b) wpływ niniejszego rozporządzenia na wykorzystywanie danych w gospodarce, w tym na innowacje w zakresie danych, monetyzację danych oraz usługi pośrednictwa danych oraz na dzielenie się danymi w ramach wspólnych europejskich przestrzeni danych;

c) dostępność i wykorzystywanie różnych kategorii i rodzajów danych;

d) wyłączenie niektórych kategorii przedsiębiorstw jako beneficjentów na mocy art. 5;

e) brak wpływu na prawa własności intelektualnej;

f) wpływ na tajemnice przedsiębiorstwa, w tym ochronę przed ich niezgodnym z prawem nabywaniem, wykorzystywaniem i ujawnianiem, oraz wpływ mechanizmu umożliwiającego posiadaczowi danych odrzucenie wniosku użytkownika na podstawie art. 4 ust. 8 i art. 5 ust. 11, przy uwzględnieniu w jak największym zakresie wszelkiej zmiany dyrektywy (UE) 2016/943;

g) czy wykaz nieuczciwych postanowień umownych, o których mowa w art. 13, jest aktualny w świetle nowych praktyk prowadzenia działalności gospodarczej i szybkiego tempa innowacji na rynku;

h) zmiany w praktykach umownych dostawców usług przetwarzania danych oraz czy prowadzi to do wystarczającego przestrzegania art. 25;

i) obniżenie opłat za proces zmiany dostawcy nakładanych przez dostawców usług przetwarzania danych, zgodnie ze stopniowym wycofywaniem opłat z tytułu zmiany dostawcy na podstawie art. 29;

j) wzajemne oddziaływanie między niniejszym rozporządzeniem a innymi aktami prawnymi Unii istotnymi dla gospodarki opartej na danych;

k) zapobieganie niezgodnemu z prawem dostępowi administracji rządowej do danych nieosobowych;

l) efektywność systemu egzekwowania przepisów wymaganego na podstawie art. 37;

m) wpływ niniejszego rozporządzenia na MŚP w odniesieniu do ich innowacyjności i do dostępności usług przetwarzania danych dla unijnych użytkowników oraz do obciążeń związanych z przestrzeganiem nowych obowiązków.

2. Do dnia ... [56 miesięcy od dnia wejścia w życie niniejszego rozporządzenia] Komisja przeprowadza ocenę niniejszego rozporządzenia i przedkłada sprawozdanie na temat jej głównych ustaleń Parlamentowi Europejskiemu i Radzie, a także Europejskiemu Komitetowi Ekonomiczno-Społecznemu. Ocena ta uwzględnia wpływ art. 23 do 31 oraz art. 34 i 35, w szczególności na wycenę i różnorodność usług przetwarzania danych oferowanych w Unii, ze szczególnym uwzględnieniem dostawców będących MŚP.

3. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania sprawozdań, o których mowa w ust. 1 i 2.

4. Na podstawie sprawozdań, o których mowa w ust. 1 i 2, Komisja może w stosownym przypadku przedłożyć Parlamentowi Europejskiemu i Radzie wniosek ustawodawczy dotyczący zmiany niniejszego rozporządzenia.

Artykuł 50

Wejście w życie i rozpoczęcie stosowania

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

Niniejsze rozporządzenie stosuje się od dnia... [20 miesięcy od dnia wejścia życie niniejszego rozporządzenia].

Obowiązki wynikające z art. 3 ust. 1 mają zastosowanie do produktów skomunikowanych i usług z nimi powiązanych wprowadzonych na rynek po dniu... [32 miesiące od dnia wejścia w życie niniejszego rozporządzenia].

Rozdział III ma zastosowanie wyłącznie do obowiązków udostępniania danych ustanowionych na mocy prawa Unii lub prawa krajowego przyjętego zgodnie z prawem Unii, które to prawo Unii lub prawo krajowe przyjęte zgodnie z prawem Unii wchodzi w życie po dniu... [20 miesięcy od dnia wejścia w życie niniejszego rozporządzenia].

Rozdział IV ma zastosowanie do umów zawartych po dniu... [20 miesięcy od dnia wejścia w życie niniejszego rozporządzenia].

Rozdział IV ma zastosowanie od dnia... [44 miesiące od dnia wejścia w życie niniejszego rozporządzenia] do umów zawartych do dnia... [20 miesięcy od dnia wejścia w życie niniejszego rozporządzenia] włącznie, pod warunkiem że:

a) zostały zawarte na czas nieokreślony; lub

b) wygasają co najmniej 10 lat po dniu... [data wejścia w życie niniejszego rozporządzenia].

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

Sporządzono w ...

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący / Przewodnicząca*