KOMISJA
EUROPEJSKA

Bruksela, dnia 23.2.2022 r.
COM(2022) 68 final

2022/0047 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych)

(Tekst mający znaczenie dla EOG)

{SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Niniejsze uzasadnienie towarzyszy wnioskowi dotyczącemu rozporządzenia w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystania (akt w sprawie danych).

Dane są kluczowym elementem gospodarki cyfrowej oraz zasobem niezbędnym do zapewnienia dwojakiej transformacji – ekologicznej i cyfrowej. W ostatnich latach ilość danych generowanych przez ludzi i maszyny gwałtownie rośnie. Większość danych jest jednak niewykorzystywana lub ich wartość skoncentrowana jest w rękach stosunkowo niewielu dużych przedsiębiorstw. Niski poziom zaufania, sprzeczne zachęty gospodarcze i bariery technologiczne utrudniają pełne wykorzystanie innowacji wykorzystujących potencjał danych. Kluczowe znaczenie ma zatem uwolnienie tego potencjału przez zapewnienie możliwości ponownego wykorzystania danych, a także przez usunięcie barier ograniczających rozwój europejskiej gospodarki opartej na danych, zgodnie z przepisami europejskimi i przy pełnym poszanowaniu wartości europejskich, a także zgodnie z misją polegającą na zmniejszeniu przepaści cyfrowej, tak aby każdy mógł skorzystać z tych możliwości. Zapewnienie większej równowagi w rozkładzie wartości danych w związku z nową falą nieosobowych danych przemysłowych oraz mnożeniem się produktów podłączonych do internetu rzeczy oznacza, że istnieje ogromny potencjał do pobudzenia zrównoważonej gospodarki opartej na danych w Europie.

Wprowadzenie przepisów dotyczących dostępu do danych i ich wykorzystania jest warunkiem wstępnym wykorzystania możliwości, jakie niesie ze sobą epoka cyfrowa, w której żyjemy. Przewodnicząca Komisji Ursula von der Leyen stwierdziła w swoich wytycznych politycznych dla Komisji na lata 2019–2024, że Europa musi „zachować równowagę między przepływem i szerokim wykorzystywaniem danych a wysokim poziomem prywatności, bezpieczeństwa i norm etycznych”[1]. W programie prac Komisji na 2020 r.[2] określono szereg celów strategicznych, w tym europejską strategię w zakresie danych[3] przyjętą w lutym 2020 r. Strategia ta jest ukierunkowana na stworzenie prawdziwie jednolitego rynku danych oraz zapewnienie Europie pozycji światowego lidera w dziedzinie gospodarki sprawnie wykorzystującej dane. Z tego powodu akt w sprawie danych jest kluczowym filarem i drugą ważną inicjatywą zapowiedzianą w strategii w zakresie danych. W szczególności akt ten przyczynia się do stworzenia międzysektorowych ram zarządzania dostępem do danych i ich wykorzystaniem przez ustanawianie przepisów dotyczących kwestii, które mają wpływ na relacje między podmiotami gospodarki opartej na danych, w celu zapewnienia zachęt do horyzontalnego udostępniania danych między sektorami.

W konkluzjach Rady Europejskiej z dnia 21–22 października 2021 r. podkreślono, „że ważne są szybkie postępy w kwestii innych bieżących i przyszłych inicjatyw, takich jak w szczególności wykorzystanie wartości danych w Europie, zwłaszcza dzięki kompleksowym ramom regulacyjnym, które będą sprzyjać innowacjom, ułatwią skuteczniejsze przenoszenie

---

[1] Ursula von der Leyen, Unia, która mierzy wyżej – Mój program dla Europy, wytyczne polityczne na następną kadencję Komisji Europejskiej (2019–2024), 16 lipca 2019 r.

[2] Komisja Europejska, załączniki do programu prac Komisji na 2020 r. – Unia, która mierzy wyżej, COM(2020) 37, 29 stycznia 2020 r.

[3] COM(2020) 66 final.

danych i sprawiedliwy dostęp do danych oraz zapewnią interoperacyjność”[4]. W dniu 25 marca 2021 r. Rada Europejska ponownie podkreśliła „znaczenie lepszego wykorzystania potencjału danych i technologii cyfrowych z pożytkiem dla społeczeństwa i gospodarki”[5]. W dniach 1–2 października 2020 r. podkreśliła, „że trzeba poprawić dostępność wysokiej jakości danych oraz promować i umożliwiać sprawniejsze wymienianie i łączenie danych, a także lepszą interoperacyjność”[6]. Jeżeli chodzi o usługi w chmurze, w dniu 15 października 2020 r. państwa członkowskie UE jednogłośnie przyjęły wspólną deklarację w sprawie budowy chmury nowej generacji dla przedsiębiorstw i sektora publicznego w UE. Będzie to wymagało stworzenia oferty dotyczącej chmury nowej generacji w UE spełniającej najwyższe standardy np. w zakresie przenoszenia danych i interoperacyjności[7].

W rezolucji Parlamentu Europejskiego z dnia 25 marca 2021 r. w sprawie europejskiej strategii w zakresie danych wezwano Komisję do przedstawienia aktu w sprawie danych, aby zachęcić do większego i sprawiedliwszego przepływu danych we wszystkich sektorach, między przedsiębiorstwami, między przedsiębiorstwami a administracją publiczną, między administracją publiczną a przedsiębiorstwami i między administracjami publicznymi, a także aby umożliwić taki przepływ[8]. W rezolucji z dnia 25 marca 2021 r. Parlament Europejski podkreślił również potrzebę stworzenia wspólnych europejskich przestrzeni danych do celów swobodnego przepływu danych nieosobowych w kontekście transgranicznym i sektorowym oraz między przedsiębiorstwami, środowiskami akademickimi, odpowiednimi zainteresowanymi stronami i sektorem publicznym. W związku z tym Parlament Europejski zachęcił Komisję do wyjaśnienia kwestii praw użytkowania, zwłaszcza w relacjach między przedsiębiorstwami i między przedsiębiorstwami a administracją publiczną. Podkreślił, że zakłócenia równowagi rynkowej wynikające z koncentracji danych ograniczają konkurencję, zwiększają bariery wejścia na rynek oraz ograniczają szerszy dostęp do danych i ich wykorzystanie.

W rezolucji Parlament Europejski podkreślił również, że ustalenia umowne między przedsiębiorstwami niekoniecznie gwarantują odpowiedni dostęp do danych dla małych i średnich przedsiębiorstw (MŚP). Powodem tego są dysproporcje pod względem siły negocjacyjnej i wiedzy fachowej. Parlament Europejski podkreśla zatem potrzebę określenia w umowach jasnych obowiązków i ustalenia odpowiedzialności w zakresie dostępu do danych, ich przetwarzania, udostępniania i przechowywania, aby ograniczyć ich niewłaściwe wykorzystywanie.

W związku z tym zwrócono się do Komisji i państw członkowskich UE o przeanalizowanie praw i obowiązków podmiotów w zakresie dostępu do danych, w których generowaniu uczestniczyły, oraz o zwiększenie ich wiedzy w szczególności na temat prawa do dostępu do danych, ich przenoszenia, wezwania innej strony do zaprzestania ich wykorzystywania, ich sprostowania lub usunięcia, przy jednoczesnym wskazaniu posiadaczy i określeniu charakteru tych praw.

---

[4] Rada Europejska, posiedzenie Rady Europejskiej (21–22 października 2021 r.) – konkluzje EUCO 17/21, 2021, s. 2.

[5] Rada Europejska, oświadczenie członków Rady Europejskiej (25 marca 2021 r.) – oświadczenie SN 18/21, s. 4.

[6] Rada Europejska, posiedzenie Rady Europejskiej (1–2 października 2020 r.) – konkluzje EUCO 13/20, 2020, s. 5.

[7] Komisja Europejska (2020). *Commission welcomes Member States' declaration on EU cloud federation* [Komisja z zadowoleniem przyjmuje deklarację państw członkowskich w sprawie federacji chmur obliczeniowych w UE], komunikat prasowy.

[8] Rezolucja Parlamentu Europejskiego z dnia 25 marca 2021 r. w sprawie europejskiej strategii w zakresie danych (2020/2217(INI)).

Jeżeli chodzi o wymianę danych między przedsiębiorstwami a organami administracji, Parlament Europejski zwrócił się do Komisji o określenie okoliczności, warunków i zachęt, w ramach których sektor prywatny powinien być zobowiązany do udostępniania danych do wykorzystania przez sektor publiczny, np. ze względu na konieczność organizacji usług publicznych opartych na danych, a także o dokonanie analizy obowiązkowych programów wymiany danych między przedsiębiorstwami a organami administracji, np. w sytuacjach, na które ludzie nie mają wpływu.

W tym kontekście Komisja przedstawia **akt w sprawie danych**, którego dotyczy niniejszy wniosek, **ukierunkowany na zapewnienie sprawiedliwego podziału wartości danych między podmiotami gospodarki opartej o dane oraz na ułatwianie dostępu do danych i ich wykorzystania**.

Niniejszy wniosek pomoże zrealizować szerzej zakrojone cele polityki polegające na zapewnieniu przedsiębiorstwom unijnym we wszystkich sektorach możliwości wprowadzania innowacji i konkurowania, skutecznym wzmocnieniu pozycji osób fizycznych w odniesieniu do ich danych oraz na zapewnieniu przedsiębiorstwom i organom sektora publicznego lepszego proporcjonalnego i przewidywalnego mechanizmu służącego rozwiązywaniu poważnych problemów politycznych i społecznych, w tym niebezpieczeństw publicznych i innych sytuacji wyjątkowych. Przedsiębiorstwa będą mogły z łatwością przenosić swoje dane i inne aktywa cyfrowe między konkurującymi ze sobą dostawcami usług w chmurze i innych usług w zakresie przetwarzania danych. Udostępnianie danych w ramach poszczególnych sektorów gospodarki i między nimi wymaga określenia ram interoperacyjności obejmujących środki proceduralne i legislacyjne w celu zwiększenia zaufania i poprawy skuteczności. Stworzenie wspólnych europejskich przestrzeni danych dla strategicznych sektorów gospodarki i dziedzin interesu publicznego przyczyni się do powstania autentycznego rynku wewnętrznego danych umożliwiającego udostępnianie danych i ich wykorzystanie we wszystkich sektorach. Niniejsze rozporządzenie przyczynia się zatem do opracowania tych ram zarządzania i infrastruktury, a także do udostępniania danych poza przestrzeniami danych.

Poniżej przedstawiono cele szczegółowe wniosku.

– **Ułatwianie dostępu do danych i ich wykorzystania przez konsumentów i przedsiębiorstwa, przy jednoczesnym zachowaniu czynników zachęcających do inwestowania w sposoby generowania wartości za pomocą danych.** Obejmuje to zwiększenie pewności prawa w zakresie udostępniania danych uzyskanych lub wygenerowanych w wyniku korzystania z produktów lub powiązanych usług, a także wdrożenie zasad w celu zapewnienia uczciwego charakteru umów dotyczących udostępniania danych. We wniosku **wyjaśniono** zastosowanie odpowiednich praw wynikających z dyrektywy 96/9/WE w sprawie ochrony prawnej baz danych (zwanej dalej **„dyrektywą w sprawie baz danych”**)[9] do jego postanowień.

– **Zapewnienie możliwości korzystania przez organy sektora publicznego oraz instytucje, agencje lub organy Unii z danych znajdujących się w posiadaniu przedsiębiorstw w określonych przypadkach wystąpienia wyjątkowej potrzeby uzyskania dostępu do danych.** Dotyczy to przede wszystkim przypadków wystąpienia niebezpieczeństwa publicznego, ale również innych sytuacji wyjątkowych, w których uzasadnione jest zastosowanie obowiązkowych programów wymiany danych między przedsiębiorstwami a organami administracji, w celu

[9] Dz.U. L 77 z 27.3.1996, s. 20.

wspierania opartych na dowodach, skutecznych, efektywnych i nastawionych na wyniki strategii i usług publicznych.

– **Ułatwianie przechodzenia od jednych do drugich usług w chmurze i usług przetwarzania brzegowego.** Dostęp do konkurencyjnych i interoperacyjnych usług przetwarzania danych jest warunkiem wstępnym pomyślnego rozwoju gospodarki opartej o dane, w której możliwe jest łatwe udostępnianie danych w ramach ekosystemów sektorowych i między nimi. Poziom zaufania do usług przetwarzania danych jest czynnikiem decydującym o wykorzystaniu tych usług przez użytkowników we wszystkich sektorach gospodarki.

– **Wdrożenie środków zabezpieczających przed bezprawnym przekazywaniem danych bez powiadomienia przez dostawców usług w chmurze**. Wynika to z faktu, że pojawiły się obawy dotyczące bezprawnego dostępu do danych przez rządy państw spoza UE / Europejskiego Obszaru Gospodarczego (EOG). Takie środki zabezpieczające powinny przyczyniać się do dalszego zwiększania zaufania do usług przetwarzania danych, na których w coraz większym stopniu opiera się europejska gospodarka oparta o dane.

– **Zapewnienie opracowania norm w zakresie interoperacyjności w odniesieniu do danych, które mają być ponownie wykorzystywane między sektorami**, w celu usunięcia barier ograniczających udostępnianie danych między wspólnymi europejskimi przestrzeniami danych w poszczególnych dziedzinach, zgodnie z sektorowymi wymogami dotyczącymi interoperacyjności, oraz między innymi danymi, które nie wchodzą w zakres określonej wspólnej europejskiej przestrzeni danych. We wniosku wspiera się również określenie norm dotyczących „inteligentnych umów". Są to programy komputerowe zapisywane w rejestrach elektronicznych, w ramach których realizuje się i rozlicza transakcje na podstawie wcześniej ustalonych warunków. Mogą one potencjalnie zagwarantować posiadaczom i odbiorcom danych przestrzeganie warunków dotyczących udostępniania danych.

• **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Niniejszy wniosek jest zgodny z obowiązującymi przepisami dotyczącymi **przetwarzania danych osobowych** (w tym z ogólnym rozporządzeniem o ochronie danych („RODO")[10]) oraz ochrony prywatności i **poufności komunikacji**, a także wszelkich danych (osobowych i nieosobowych) przechowywanych w urządzeniach końcowych i uzyskiwanych za ich pośrednictwem (dyrektywą o e-prywatności[11], którą zastąpi rozporządzenie o e-prywatności będące obecnie przedmiotem negocjacji legislacyjnych). Niniejszy wniosek stanowi uzupełnienie istniejących praw, szczególnie praw dotyczących danych generowanych przez produkt użytkownika podłączony do publicznej sieci łączności elektronicznej.

W **rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych**[12] ustanowiono kluczowy element europejskiej gospodarki opartej o dane przez zapewnienie możliwości przechowywania, przetwarzania i przekazywania danych nieosobowych w dowolnym miejscy w Unii. Przedstawiono w nim również samoregulacyjne podejście do problemu uzależnienia od jednego dostawcy na poziomie dostawców usług przetwarzania danych przez wprowadzenie kodeksów postępowania ułatwiających zmianę dostawców usług w chmurze (kodeksy postępowania w zakresie „zmiany dostawców usług w chmurze

10 Dz.U. L 119 z 4.5.2016, s. 1.
11 Dz.U. L 201 z 31.7.2002, s. 37.
12 Dz.U. L 303 z 28.11.2018, s. 59; SWIPO (2021), zob. *strona internetowa*.

i przenoszenia danych (SWIPO)" opracowane przez branżę). Niniejszy wniosek opiera się na tych elementach i pomaga przedsiębiorstwom i obywatelom w możliwie najskuteczniejszym wykorzystaniu prawa do zmiany dostawcy danych w chmurze i przenoszenia danych. Jest on również w pełni zgodny z dyrektywą w sprawie nieuczciwych postanowień umownych, jeżeli chodzi o prawo zobowiązań[13]. W odniesieniu do usług w chmurze, ponieważ wydaje się, że samoregulacyjne podejście nie wpłynęło znacząco na dynamikę rynku, w niniejszym wniosku przedstawiono podejście regulacyjne do problemu, na który zwrócono uwagę w rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych.

Kwestie dotyczące przetwarzania i przechowywania danych na szczeblu międzynarodowym oraz przekazywania danych regulują przepisy RODO, zobowiązania handlowe Światowej Organizacji Handlu (WTO), Układ ogólny w sprawie handlu usługami (GATS) i dwustronne umowy handlowe.

Prawo konkurencji[14] ma zastosowanie m.in. w kontekście kontroli połączeń, udostępniania danych przez przedsiębiorstwa lub nadużywania przez nie pozycji dominującej.

W **dyrektywie w sprawie baz danych**[15] przewidziano ochronę *sui generis* baz danych, które powstały w wyniku znaczącej inwestycji, nawet w przypadku gdy sama baza danych nie jest oryginalną twórczością intelektualną chronioną prawem autorskim. W oparciu o bogate orzecznictwo stanowiące wykładnię przepisów dyrektywy w sprawie baz danych niniejszy wniosek dotyczy trwającej niepewności prawa co do tego, czy bazom danych zawierającym dane wygenerowane lub uzyskane w wyniku korzystania z produktów lub powiązanych usług, takich jak czujniki, lub innym rodzajom danych generowanych maszynowo przysługiwałaby taka ochrona.

W ramach **rozporządzenia w sprawie platform dla przedsiębiorstw**[16] nakłada się obowiązki w zakresie przejrzystości, zgodnie z którymi platformy muszą dostarczyć użytkownikom biznesowym opis danych generowanych w wyniku świadczenia usługi.

W **dyrektywie w sprawie otwartych danych**[17] określono minimalne przepisy dotyczące ponownego wykorzystywania danych będących w posiadaniu sektora publicznego oraz danych badawczych finansowanych ze środków publicznych udostępnianych publicznie za pośrednictwem repozytoriów.

Inicjatywa na rzecz interoperacyjnej Europy jest ukierunkowana na wprowadzenie polityki w zakresie interoperacyjności opartej na współpracy w odniesieniu do zmodernizowanego sektora publicznego. Inicjatywa powstała w ramach programu ISA^2, unijnego programu finansowania realizowanego w latach 2016–2021 i wspierającego rozwój rozwiązań cyfrowych umożliwiających świadczenie interoperacyjnych transgranicznych i międzysektorowych usług publicznych[18].

Niniejszy wniosek stanowi uzupełnienie niedawno przyjętego **aktu w sprawie zarządzania danymi** ukierunkowanego na ułatwienie dobrowolnego udostępniania danych przez osoby fizyczne i przedsiębiorstwa oraz harmonizującego warunki wykorzystywania określonych danych sektora publicznego, bez zmieniania praw materialnych dotyczących danych ani

13 Dz.U. L 95 z 21.4.1993, s. 29.
14 Dz.U. L 335 z 18.12.2010, s. 36.
15 Dz.U. L 77 z 27.3.1996, s. 20.
16 Dz.U. L 186 z 11.7.2019, s. 57.
17 Dz.U. L 172 z 26.6.2019, s. 56.
18 Dz.U. L 318 z 4.12.2015, s. 1.

ustanowionych praw dostępu do danych i ich wykorzystania[19]. Ponadto stanowi on uzupełnienie wniosku dotyczącego **aktu o rynkach cyfrowych**, w ramach którego określeni dostawcy podstawowych usług platformowych określanych jako „strażnicy dostępu" będą zobowiązani do zapewnienia skuteczniejszego przenoszenia danych generowanych w wyniku działalności przedsiębiorstw i użytkowników końcowych[20].

Niniejszy wniosek nie ma wpływu na obowiązujące przepisy w dziedzinie własności intelektualnej (z wyjątkiem stosowania prawa *sui generis* określonego w dyrektywie w sprawie baz danych), konkurencji, wymiaru sprawiedliwości i spraw wewnętrznych oraz związanej z nimi współpracy (międzynarodowej), zobowiązań handlowych lub ochrony prawnej tajemnic przedsiębiorstwa.

W szeregu obszarów konieczne jest dostosowanie prawa w celu promowania transformacji cyfrowej. W ramach europejskiego cyfrowego paszportu produktu (jako część inicjatywy na rzecz zrównoważonych produktów) zostaną ustanowione jasne zasady dostępu do konkretnych danych niezbędnych do zapewnienia zamkniętego cyklu życia i zrównoważonego charakteru określonych produktów w całym ich cyklu życia oraz w sytuacjach niebędących wyjątkowymi[21]. Przepisy prawa prywatnego stanowią kluczowy element ogólnie rozumianych ram. W ramach niniejszego rozporządzenia dostosowuje się zatem prawo zobowiązań i inne przepisy, aby poprawić warunki ponownego wykorzystywania danych na rynku wewnętrznym oraz zapobiec nadużywaniu przez strony umów braku równowagi pod względem pozycji negocjacyjnej ze szkodą dla słabszych stron.

W **akcie w sprawie danych**, jako wniosku horyzontalnym, przewidziano **podstawowe zasady w odniesieniu do wszystkich sektorów** w zakresie praw do wykorzystywania danych, np. w dziedzinie inteligentnych maszyn lub dóbr konsumpcyjnych. Prawa i obowiązki w zakresie dostępu do danych i ich wykorzystywania uregulowano jednak również w różnym stopniu na poziomie sektorowym. Na mocy aktu w sprawie danych nie zostaną zmienione żadne z takich obowiązujących przepisów, ale przyszłe przepisy w tych dziedzinach należy co do zasady dostosować do zasad horyzontalnych określonych w akcie w sprawie danych. Podczas przeglądu instrumentów sektorowych należy ocenić zbieżność z zasadami horyzontalnymi określonymi w akcie w sprawie danych. W niniejszym wniosku pozostawiono miejsce dla prawodawstwa pionowego w celu określenia bardziej szczegółowych zasad dotyczących osiągnięcia sektorowych celów regulacyjnych.

Biorąc pod uwagę obowiązujące przepisy sektorowe, w odniesieniu do tworzenia przestrzeni danych dotyczących Zielonego Ładu, przegląd[22] **dyrektywy INSPIRE**[23] umożliwi dalszą otwartą dostępność i ponowne wykorzystanie danych przestrzennych i środowiskowych. Inicjatywa ta jest ukierunkowana na ułatwienie unijnym organom publicznym, przedsiębiorstwom i obywatelom wspierania przejścia na bardziej ekologiczną i bezemisyjną gospodarkę oraz zmniejszenie obciążenia administracyjnego. Oczekuje się, że wesprze ona usługi wykorzystujące dane wielokrotnego użytku na dużą skalę, tak aby wspomagać gromadzenie, wymianę, przetwarzanie i analizę dużych zbiorów danych istotnych dla zapewnia zgodności z przepisami w dziedzinie ochrony środowiska i priorytetowymi działaniami Europejskiego Zielonego Ładu. Usprawni sprawozdawczość oraz ograniczanie

19 COM(2020) 767 final.
20 Dz.U. L 186 z 11.7.2019, s. 57.
21 COM(2020) 98 final.
22 Inicjatywa „GreenData4All" (REFIT) | Legislacyjny rozkład jazdy | Parlament Europejski (europa.eu).
23 Dz.U. L 108 z 25.4.2007, s. 1.

obciążeń poprzez lepsze wielokrotne wykorzystywanie istniejących danych i automatyczne generowanie sprawozdań w drodze eksploracji danych i wywiadu gospodarczego.

Unijne **rozporządzenie w sprawie energii elektrycznej**[24] zawiera wymóg, zgodnie z którym operatorzy systemu przesyłowego muszą przekazać dane organom regulacyjnym oraz na potrzeby planowania w zakresie wystarczalności zasobów, natomiast w unijnej **dyrektywie w sprawie energii elektrycznej**[25] przewidziano przejrzysty i niedyskryminujący dostęp do danych oraz upoważniono Komisję do opracowania odpowiednich wymogów i procedur dotyczących interoperacyjności w celu ułatwienia tego procesu. W ramach **drugiej dyrektywy w sprawie usług płatniczych**[26] otwiera się, pod pewnymi warunkami, dostęp do niektórych rodzajów informacji na temat transakcji płatniczych i informacji księgowych, umożliwiając w ten sposób udostępnianie danych między przedsiębiorstwami w obszarze technologii finansowej. W sektorze mobilności i transportu obowiązuje wiele różnych zasad dostępu do danych i ich udostępniania. Informacje dotyczące naprawy i konserwacji pojazdów silnikowych i maszyn rolniczych podlegają szczególnym zobowiązaniom w zakresie dostępu do danych / udostępniania danych na podstawie **przepisów dotyczących homologacji typu**[27]. Potrzebne są jednak nowe przepisy w celu zapewnienia, aby obowiązujące przepisy dotyczące homologacji typu całego pojazdu były dostosowane do epoki cyfrowej i wspierały rozwój czystych ekologicznie, zautomatyzowanych pojazdów podłączonych do internetu. W oparciu o akt w sprawie danych, który stanowi ramy dotyczące dostępu do danych i ich wykorzystania, przepisy te będą dotyczyć wyzwań charakterystycznych dla danego sektora, w tym dostępu do funkcji i zasobów pojazdów.

W ramach **dyrektywy w sprawie inteligentnych systemów transportowych**[28] opracowano szereg rozporządzeń delegowanych, które będą nadal opracowywane, zwłaszcza w celu określenia dostępności danych na potrzeby drogowego i multimodalnego transportu pasażerskiego, w szczególności za pośrednictwem krajowych punktów dostępu. W przypadku zarządzania ruchem lotniczym dane nieoperacyjne mają istotne znaczenie dla poprawy intermodalności i łączności. Dane operacyjne związane z zarządzaniem ruchem lotniczym podlegałyby szczególnemu systemowi określonemu w ramach **jednolitej europejskiej przestrzeni powietrznej**[29]. W przypadku monitorowania ruchu statków dane dotyczące statków (ich śledzenia i namierzania) mają istotne znaczenie dla poprawy intermodalności i łączności: dane te są objęte szczególnym systemem określonym w dyrektywie w sprawie VTMIS[30]. Ponadto wchodzą one w zakres stosowania cyfrowego systemu morskiego i cyfrowych usług morskich[31]. We wniosku dotyczącym rozporządzenia w sprawie rozwoju **infrastruktury paliw alternatywnych**[32] określono odpowiednie rodzaje danych, które mają być udostępniane, w synergii z ogólnymi ramami ustanowionymi w dyrektywie w sprawie inteligentnych systemów transportowych.

- **Spójność z innymi politykami Unii**

Niniejszy wniosek jest zgodny z priorytetami Komisji dotyczącymi **stworzenia Europy na**

24 Dz.U. L 158 z 14.6.2019, s. 54.
25 Dz.U. L 158 z 14.6.2019, s. 125.
26 Dz.U. L 337 z 23.12.2015, s. 35, Dz.U. L 337 z 23.12.2015, s. 35.
27 Dz.U. L 151 z 14.6.2018, s. 1; Dz.U. L 60 z 2.3.2013, s. 1.
28 Dz.U. L 207 z 6.8.2010, s. 1.
29 Dz.U. L 96 z 31.3.2004, s. 1; Dz.U. L 96 z 31.3.2004, s. 10; Dz.U. L 96 z 31.3.2004, s. 20.
30 Dz.U. L 308 z 29.10.2014, s. 82.
31 Dz.U. L 96 z 12.4.2016, s. 46.
32 COM(2021) 559 final.

miarę ery cyfrowej i zbudowania gospodarki gotowej na przyszłe wyzwania, która będzie przynosić korzyści obywatelom[33], gdzie transformację cyfrową rynku wewnętrznego będzie charakteryzować wysoki poziom zaufania, bezpieczeństwa, ochrony i wyboru dla konsumentów. Transformacja cyfrowa rynku wewnętrznego jest wysoce konkurencyjna dzięki ramom, które sprzyjają przejrzystości, konkurencji i innowacjom oraz są neutralne pod względem technologicznym. Stanowi ona wsparcie dla **Instrumentu na rzecz Odbudowy i Zwiększania Odporności**[34] dzięki wnioskom wyciągniętym z pandemii COVID-19 oraz korzyściom płynącym z łatwiejszego dostępu do danych w razie potrzeby.

W niniejszym wniosku na różne sposoby wspiera się kluczową rolę danych w osiąganiu celów przewidzianych w **Europejskim Zielonym Ładzie**. Po pierwsze, poprzez lepsze zrozumienie przez rządy, przedsiębiorstwa i osoby fizyczne wpływu, jaki produkty, usługi i materiały w całym łańcuchu dostaw wywierają na społeczeństwo i gospodarkę. Po drugie, przez wykorzystanie istniejącego bogactwa odpowiednich danych sektora prywatnego w celu rozwiązania problemów związanych z klimatem, bioróżnorodnością, zanieczyszczeniem[35] i zasobami naturalnymi zgodnie z celami określonymi w Europejskim Zielonym Ładzie[36], odpowiednimi konkluzjami Rady[37] oraz stanowiskami[38] Parlamentu Europejskiego. Po trzecie, przez uzupełnienie luk w wiedzy i zarządzanie związanymi z tym kryzysami za pomocą bardziej intensywnych działań w zakresie łagodzenia skutków, gotowości, reagowania i odbudowy.

Zgodnie ze **strategią przemysłową**[39] wniosek dotyczy technologii o ogromnym znaczeniu strategicznym, takich jak przetwarzanie w chmurze i systemy sztucznej inteligencji: obszarów, których pełnego potencjału UE jeszcze nie wykorzystała, a które znajdują się u progu kolejnej fali danych przemysłowych. W ramach wniosku realizowany jest cel określony w **strategii w zakresie danych**[40] polegający na poprawie zdolności przedsiębiorstw do wprowadzania innowacji i konkurowania w oparciu o wartości UE, oraz zasada **swobodnego przepływu danych na rynku wewnętrznym**. Jest on również zgodny z **planem działania w zakresie własności intelektualnej**[41], w którym Komisja zobowiązała się do dokonania przeglądu dyrektywy w sprawie baz danych.

Niniejszy wniosek powinien być również zgodny z zasadami określonymi w Planie działania na rzecz Europejskiego filaru praw socjalnych[42] oraz z wymogami dostępności określonymi w dyrektywie (UE) 2019/882 w sprawie wymogów dostępności produktów i usług[43].

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawę prawną niniejszego wniosku stanowi art. 114 Traktatu o funkcjonowaniu Unii

---

33 COM(2020) 67 final.
34 Dz.U. L 57 z 18.2.2021, s. 17.
35 COM(2021) 400 final.
36 COM(2019) 640 final.
37 Cyfryzacja na rzecz środowiska, 11 grudnia 2020 r., konkluzje Rady w sprawie nowego planu działania dotyczącego gospodarki o obiegu zamkniętym, 11 grudnia 2020 r., konkluzje Rady w sprawie a strategii na rzecz bioróżnorodności 2030, 16 października 2020 r., konkluzje w sprawie poprawy jakości powietrza, 5 marca 2020 r.
38 Alarmująca sytuacja klimatyczna i środowiskowa – czwartek, 28 listopada 2019 r. (europa.eu).
39 COM(2021) 350 final.
40 COM(2020) 66 final.
41 COM(2020) 760 final.
42 COM(2021) 102 final.
43 Dz.U. L 151 z 7.6.2019.

Europejskiej, którego celem jest ustanowienie i funkcjonowanie rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych.

Celem niniejszego wniosku jest zakończenie procesu tworzenia rynku wewnętrznego danych, na którym dane pochodzące z sektora publicznego, przedsiębiorstw i od osób fizycznych są wykorzystywane w najlepszy możliwy sposób, przy jednoczesnym poszanowaniu praw związanych z takimi danymi i inwestycjami poczynionymi w celu ich gromadzenia. Przepisy dotyczące zmiany dostawców usług w zakresie przetwarzania danych są ukierunkowane na ustanowienie sprawiedliwych i konkurencyjnych warunków rynkowych w odniesieniu do rynku wewnętrznego usług w chmurze, usług przetwarzania brzegowego i powiązanych usług.

Ochrona poufnych danych przedsiębiorstwa i tajemnicy przedsiębiorstwa jest ważnym aspektem sprawnego funkcjonowania rynku wewnętrznego, podobnie jak w przypadku innych kontekstów, w których odbywa się wymiana usług i towarów. W niniejszym wniosku zawarto przepisy gwarantujące poszanowanie tajemnic przedsiębiorstwa w kontekście wykorzystywania danych między przedsiębiorstwami lub przez konsumentów. Inicjatywa zapewni Unii możliwość czerpania korzyści wynikających ze skali rynku wewnętrznego, ponieważ produkty lub powiązane usługi są często opracowywane z wykorzystaniem danych pochodzących z różnych państw członkowskich, a następnie komercjalizowane na terytorium całej Unii.

Niektóre państwa członkowskie podjęły działania legislacyjne, aby rozwiązać opisane powyżej problemy w ramach scenariuszy dotyczących relacji między przedsiębiorstwami i w ramach scenariuszy dotyczących relacji między przedsiębiorstwami a administracją publiczną, podczas gdy inne tego nie zrobiły. Może to doprowadzić do rozdrobnienia legislacyjnego na rynku wewnętrznym oraz do stosowania różnych przepisów i praktyk w Unii, co z kolei wiązałoby się z koniecznością ponoszenia dodatkowych kosztów przez przedsiębiorstwa, które byłyby zobowiązane do zapewniania zgodności z różnymi systemami. Dlatego też należy zapewnić spójne stosowanie proponowanych środków we wszystkich państwach członkowskich.

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

Biorąc pod uwagę transgraniczny charakter procesu wykorzystywania danych oraz mnogość obszarów, na które akt w sprawie danych wywiera wpływ, kwestie będące przedmiotem niniejszego wniosku nie mogą zostać skutecznie rozstrzygnięte na szczeblu państwa członkowskiego. Należy unikać rozdrobnienia wynikającego z różnic między przepisami krajowymi, ponieważ mogłoby ono doprowadzić do wyższych kosztów transakcyjnych, braku przejrzystości, niepewności prawa i niepożądanej „turystyki sądowej”. Niedopuszczenie do takiego rozdrobnienia ma szczególnie istotne znaczenie we wszystkich sytuacjach dotyczących powiązanych z danymi aspektów relacji między przedsiębiorstwami, uwzględniając uczciwe postanowienia i zobowiązania umowne producentów produktów internetu rzeczy lub powiązanych usług, które to aspekty wymagają zapewnienia homogeniczności ram w całej Unii.

Wyniki oceny transgranicznych aspektów przepływów danych w obszarze wymiany danych między przedsiębiorstwami a organami administracji również wskazują na konieczność podjęcia działań na szczeblu Unii. Dużą część podmiotów prywatnych, które dysponują odpowiednimi danymi, stanowią korporacje wielonarodowe. Wspomniane korporacje nie powinny być zmuszane do konfrontowania się z rozdrobnionym systemem prawnym.

Usługi w chmurze rzadko oferuje się wyłącznie w jednym państwie członkowskim. Zgodnie z przepisami RODO i przepisami rozporządzenia w sprawie swobodnego przepływu danych nieosobowych, które zapewniają konsumentom i przedsiębiorstwom możliwość przetwarzania danych osobowych i danych nieosobowych w dowolnym miejscu na terytorium Unii, transgraniczne przetwarzanie danych w Unii ma kluczowe znaczenie dla prowadzenia działalności gospodarczej na rynku wewnętrznym. Dlatego też należy zagwarantować stosowanie przepisów regulujących kwestie związane ze zmianą usług przetwarzania danych na szczeblu Unii, aby nie dopuścić do szkodliwego rozdrobnienia na jednolitym pod innymi względami rynku usług przetwarzania danych.

Cele wyznaczone w niniejszym wniosku – w tym utworzenie innowacyjnych i konkurencyjnych równych warunków działania dla przedsiębiorstw opartych na danych oraz wzmocnienie pozycji obywateli – można zrealizować wyłącznie poprzez podjęcie wspólnego działania na szczeblu Unii. To wspólne działanie stanowi zdecydowany krok naprzód ku realizacji wizji zakładającej utworzenie autentycznego rynku wewnętrznego danych.

- **Proporcjonalność**

W niniejszym wniosku dąży się do zrównoważenia praw i interesów dotkniętych nim zainteresowanych stron z ogólnym celem polegającym na ułatwieniu wielu różnym podmiotom szerszego korzystania z danych. Tworzy on ramy wspomagające, które nie wykraczają poza to, co jest konieczne do osiągnięcia tych celów. Odniesiono się w nim do istniejących barier utrudniających pełniejsze wykorzystanie potencjalnej wartości danych przez przedsiębiorstwa, konsumentów i organy sektora publicznego. Ustanowiono w nim również ramy na potrzeby przyszłych przepisów sektorowych, aby nie dopuścić do rozdrobnienia i niepewności prawa. Doprecyzowano w nim istniejące prawa i – w stosownych przypadkach – zagwarantowano prawa dostępu do danych, wnosząc tym samym wkład w rozwój rynku wewnętrznego usług udostępniana danych. Inicjatywa zapewnia znaczną dozę elastyczności, jeżeli chodzi o możliwość stosowania przewidzianych w niej ustaleń na poziomie sektorowym.

Niniejszy wniosek będzie wiązał się z kosztami finansowymi i administracyjnymi. Przewiduje się, że koszty te zostaną poniesione głównie przez organy krajowe, producentów i dostawców usług w związku z koniecznością wywiązania się z zobowiązań przewidzianych w przedmiotowym rozporządzeniu. Analiza różnych wariantów oraz ich przewidywanych kosztów i korzyści z nimi związanych pozwoliła jednak opracować zrównoważony projekt instrumentu. Podobnie koszty dla użytkowników i posiadaczy danych będą zrównoważone wartością uzyskaną dzięki szerszemu dostępowi do danych i szerszemu ich wykorzystywaniu, jak również dzięki upowszechnieniu nowych usług na rynku.

- **Wybór instrumentu**

Wybór rozporządzenia jako instrumentu prawnego jest uzasadniony, ponieważ rozporządzenie stanowi najlepszy mechanizm pozwalający zrealizować szerzej zakrojone cele polityki polegające na zapewnieniu wszystkim przedsiębiorstwom w Unii możliwości wprowadzania innowacji i konkurowania, umożliwieniu konsumentom lepszego kontrolowania ich danych oraz zagwarantowaniu, aby instytucje, agencje i organy Unii były lepiej przygotowane do radzenia sobie z poważnymi wyzwaniami politycznymi, uwzględniając niebezpieczeństwa publiczne. Przyjęcie rozporządzenia jest konieczne, biorąc pod uwagę leżący u podstaw niniejszego wniosku cel zakładający kompleksową harmonizację przepisów, która ma zapewnić pewność prawa i przejrzystość dla podmiotów gospodarczych – uwzględniając mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa – a także zagwarantować osobom prawnym i fizycznym we wszystkich państwach członkowskich taki

sam poziom prawnie egzekwowalnych praw oraz obowiązków, aby zapewnić spójne egzekwowanie przepisów we wszystkich państwach członkowskich, jak również skuteczną współpracę między właściwymi organami różnych państw członkowskich.

Wniosek wzmocni rynek wewnętrzny danych poprzez zwiększenie pewności prawa i zagwarantowanie ustanowienia jednolitych, horyzontalnych i spójnych ram prawnych.

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

• Oceny *ex post*/oceny adekwatności obowiązującego prawodawstwa

Niniejszy wniosek opiera się częściowo na wynikach ostatniej oceny dyrektywy w sprawie baz danych oraz wynikach badania Komisji przeprowadzonego na potrzeby przeglądu tej dyrektywy[44]. W dyrektywie w sprawie baz danych wprowadzono m.in. konkretne prawo *sui generis* do ochrony baz danych, jeżeli twórca danej bazy danych dokonał istotnej inwestycji w pozyskanie, zweryfikowanie i przedstawienie danych znajdujących się w tej bazie. Od jej pierwotnego przyjęcia dyrektywa była dwukrotnie poddawana ocenie. Obydwie te oceny zostały uzupełnione komunikatami Komisji dotyczącymi polityki w zakresie gospodarki opartej o dane[45].

Trybunał Sprawiedliwości Unii Europejskiej doprecyzował znaczenie pojęcia istotnych inwestycji w bazę danych, wyjaśniając, że celem prawa *sui generis* jest ochrona inwestycji związanych z gromadzeniem danych, a nie ich tworzeniem[46] jako produktu ubocznego innego rodzaju działalności gospodarczej. Wciąż brak jest jednak pewności co do trybu postępowania w sytuacji przypadkowego lub niezamierzonego zastosowania prawa *sui generis* do baz danych zawierających dane generowane maszynowo, tj. dane pozyskane za pośrednictwem lub wygenerowane przy wykorzystaniu produktów lub powiązanych usług. Należy zrównoważyć cele polityki w zakresie ochrony praw własności intelektualnej do takich baz danych w kontekście gospodarki opartej o dane, biorąc pod uwagę fakt, że wyłączność takich danych jako dobra nierywalizacyjnego postrzega się zasadniczo jako przeszkodę dla innowacyjności. Aby zapewnić spójność z interwencjami regulacyjnymi zaproponowanymi w niniejszym wniosku, interwencja dotycząca prawa *sui generis* służy w szczególności rozwiązaniu zidentyfikowanego problemu związanego ze stosowaniem prawa *sui generis* w kontekście internetu rzeczy. Komisja przygotowuje również obecnie ocenę rozporządzenia (UE) 2018/1807 – oczekuje się, że wyniki tej oceny zostaną przedstawione w listopadzie 2022 r. Ze wstępnych doniesień wykonawców zewnętrznych wynika, że kodeksy postępowania SWIPO wywarły ograniczony wpływ na zjawisko zmiany dostawcy usług w chmurze.

• Konsultacje z zainteresowanymi stronami

W trakcie kadencji Komisji w jej poprzednim składzie osobowym rozpoczęto szeroko zakrojone prace mające na celu zidentyfikowanie problemów uniemożliwiających Unii pełne wykorzystanie innowacji wykorzystujących potencjał danych w gospodarce. Niniejszy wniosek bazuje na wynikach konsultacji przeprowadzonych w przeszłości, m.in. na

---

[44] COM(2017) 9 final; SWD(2018) 146 final, sekcja 5.4.2; badanie służące wsparciu oceny skutków przeprowadzanej na potrzeby przeglądu dyrektywy w sprawie baz danych.

[45] COM(2017) 9 final; COM(2020) 66 final; COM(2020) 760 final.

[46] Wyrok z dnia 9 listopada 2004 r., Fixtures Marketing Ltd/Oy Veikkaus Ab, C-46/02, wyrok z dnia 9 listopada 2004 r., Fixtures Marketing Ltd/Svenska Spel Ab, C-338/02, wyrok z dnia 9 listopada 2004 r., British Horseracing Board Ltd/William Hill, C-203/02, wyrok z dnia 9 listopada 2004 r., Fixtures Marketing Ltd/OPAP, C-444/02.

konsultacjach publicznych z 2017 r. związanych z komunikatem Komisji pt. „Budowa europejskiej gospodarki opartej na danych”[47], konsultacjach publicznych z 2017 r. dotyczących oceny dyrektywy w sprawie baz danych, konsultacjach publicznych z 2018 r. dotyczących przeglądu dyrektywy w sprawie ponownego wykorzystywania informacji sektora publicznego, konsultacji w ramach panelu MŚP z 2018 r. dotyczących zasad i wytycznych w zakresie udostępniania danych między przedsiębiorstwami oraz zorganizowanych przez Komisję otwartych konsultacji internetowych poświęconych europejskiej strategii w zakresie danych[48], które odbywały się w okresie od lutego do maja 2020 r.

28 maja 2021 r. na portalu „Lepsze stanowienie prawa” opublikowano wstępną ocenę skutków i wyznaczono termin 4 tygodni na przekazywanie informacji zwrotnych dotyczących tej oceny. Komisja otrzymała 91 uwag za pośrednictwem portalu „Lepsze stanowienie prawa”[49], które pochodziły głównie od przedsiębiorstw.

Następnie, 3 czerwca 2021 r., opublikowano zaproszenie do udziału w internetowych konsultacjach publicznych dotyczących aktu w sprawie danych. Konsultacje te zakończyły się 3 września 2021 r. Zagadnienia będące przedmiotem niniejszej inicjatywy znalazły odzwierciedlenie w poszczególnych częściach konsultacji i w pytaniach zadawanych w ich trakcie. Konsultacje były skierowane do wszystkich rodzajów zainteresowanych stron, a w ich toku gromadzono informacje dotyczące udostępniania danych, dostępu do danych oraz wykorzystywania danych w relacjach między przedsiębiorstwami oraz w relacjach między przedsiębiorstwami a administracją publiczną, informacje dotyczące wzmacniania pozycji konsumentów i możliwości przenoszenia danych, informacje na temat potencjalnej roli środków technicznych takich jak inteligentne umowy, informacje dotyczące zdolności użytkowników do zmiany usług w chmurze, informacje o prawach własności intelektualnej (a więc informacje dotyczące ochrony baz danych) oraz informacje dotyczące gwarancji dla danych nieosobowych w kontekście międzynarodowym. Po przeprowadzeniu dogłębnej analizy otrzymanych odpowiedzi Komisja opublikowała sprawozdanie podsumowujące na swojej stronie internetowej[50].

Łącznie otrzymano 449 odpowiedzi z 32 państw. Największa liczba odpowiedzi pochodziła od podmiotów gospodarczych – stowarzyszenia przedsiębiorców przekazały 122 uwagi, natomiast przedsiębiorstwa/organizacje biznesowe – 105 uwag. Ponadto 100 respondentów było organami publicznymi, a 58 osobami fizycznymi reprezentującymi opinię publiczną. Ogólnie rzecz biorąc, odpowiedzi potwierdziły istnienie całej rzeszy przeszkód utrudniających skuteczne i efektywne udostępnianie danych we wszelkiego rodzaju relacjach związanych z danymi.

W kontekście relacji między przedsiębiorstwami, mimo że udostępnianie danych między przedsiębiorstwami stanowi powszechną praktykę, respondenci, którzy napotkali trudności w tym zakresie, zwrócili uwagę na przeszkody takie jak przeszkody o charakterze technicznym (formaty, brak standardów – 69 %); bezpośrednia odmowa udzielenia dostępu do danych niepowiązana z kwestiami dotyczącymi konkurencji (55 %) lub nadużywanie nierównowagi umownej (44 %). Jeżeli chodzi o kwestie związane z umowami, prawie połowa

47 COM(2017) 9 final.

48 Komisja Europejska (2020). *Wyniki konsultacji internetowych poświęconych europejskiej strategii w zakresie danych.*

49 *Strona internetowa* Komisji Europejskiej: *Wyraź swoją opinię! Akt w sprawie danych oraz zmienione przepisy dotyczące ochrony prawnej baz danych.*

50 Komisja Europejska (2021). *Konsultacje publiczne dotyczące aktu w sprawie danych: sprawozdanie podsumowujące*.

respondentów opowiedziała się za wprowadzeniem analizy nieuczciwego charakteru (46 %), podczas gdy ponad dwukrotnie mniejsza liczba respondentów była przeciwna wprowadzeniu takiej analizy (21 %). MŚP zdecydowanie poparły wprowadzenie analizy nieuczciwego charakteru (50 %); znaczna część dużych przedsiębiorstw również opowiedziała się za tym rozwiązaniem (41 %). Podobnie 46 % zainteresowanych stron z różnych sektorów wyraziło swoje poparcie dla przyjęcia przepisów dotyczących ogólnego prawa dostępu na sprawiedliwych, rozsądnych i niedyskryminujących warunkach (46 %). 60 % respondentów – w szczególności MŚP i mikroprzedsiębiorstwa (78 %) – zgodziło się z twierdzeniem, że opracowanie modelowych postanowień umownych mogłoby przyczynić się do poprawy zwiększenia ilości udostępnianych danych. 70 % zainteresowanych stron wyraziło opinię, że w przypadku danych generowanych w kontekście internetu rzeczy można zaobserwować problem związany z uczciwością oraz że producenci produktów skomunikowanych lub powiązanych usług nie powinni być uprawnieni do jednostronnego decydowania o dalszym losie danych wygenerowanych przez takie produkty. 79 % respondentów uznało, że inteligentne umowy mogłyby stanowić skuteczne narzędzie umożliwiające techniczne wdrożenie rozwiązań w zakresie dostępu do danych i wykorzystania danych w kontekście danych współgenerowanych w ramach internetu rzeczy.

Wśród głównych czynników utrudniających wymianę danych między przedsiębiorstwami a organami administracji respondenci wymieniali niepewność prawa i przeszkody prawne, czynniki zniechęcające o charakterze komercyjnym oraz brak odpowiedniej infrastruktury. Niemal wszystkie organy publiczne uważają, że podjęcie działań (na szczeblu unijnym lub na szczeblu państwa członkowskiego) w kwestii wymiany danych między przedsiębiorstwami a organami administracji jest konieczne – w przypadku instytucji akademickich/badawczych opinię tę podziela 80 % respondentów, natomiast wśród przedsiębiorstw lub organizacji/stowarzyszeń biznesowych – 38 % respondentów. Zdecydowana większość zainteresowanych stron (w szczególności obywatele i przedstawiciele organów administracji publicznej) wyraziła również opinię, zgodnie z którą wymiana danych między przedsiębiorstwami a organami administracji powinna być obowiązkowa i obwarowana konkretnymi gwarancjami dotyczącymi określonych przypadków użycia, które ewidentnie leżą w interesie publicznym, takich jak przypadki związane z sytuacjami wyjątkowymi i zarządzaniem kryzysowym, statystyka publiczna, ochrona środowiska oraz ogólnie rozumiane działania przyczyniające się do budowania zdrowszego społeczeństwa.

Respondenci potwierdzili również przydatność rozwiązania polegającego na przyznaniu użytkownikom biznesowym prawa do przechodzenia na inne usługi przetwarzania w chmurze. Jeżeli chodzi o gwarancje dotyczące danych nieosobowych w kontekstach międzynarodowych, 76 % respondentów postrzega możliwość uzyskania dostępu do danych przez organy państwa trzeciego na podstawie przepisów prawa obcego jako ryzyko dla swojej organizacji, przy czym 19 % z nich traktuje taką możliwość jako poważne ryzyko.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Wniosek sporządzono w oparciu o wyniki szeregu badań, warsztatów i innego rodzaju opinii eksperckich:

– **Badanie służące wsparciu oceny skutków dotyczące zwiększania stopnia wykorzystania danych w Europie**, w ramach którego odbyto rozmowy z określonymi zainteresowanymi stronami. Badanie to obejmowało międzysektorowe warsztaty poświęcone problematyce wymiany danych między przedsiębiorstwami i wymiany danych między przedsiębiorstwami a organami

administracji, jak również ostateczne warsztaty walidacyjne zorganizowane wiosną 2021 r.

– **W ramach badania dotyczącego modelowych postanowień umownych, kontroli uczciwości w dziedzinie udostępniania danych i w obszarze umów dotyczących usług w chmurze oraz praw dostępu do danych** oceniono w szczególności powiązane z uczciwością aspekty udostępniania danych w relacjach między przedsiębiorstwami; badanie to obejmowało również ukierunkowane rozmowy z zainteresowanymi stronami i warsztaty walidacyjne.

– **Badanie na temat szkód gospodarczych wynikających z nieuczciwych i nierównych umów o przetwarzanie w chmurze**. Badanie to obejmowało ankietę internetową z udziałem wybranych MŚP i przedsiębiorstw typu start-up korzystających z usług przetwarzania w chmurze do prowadzenia swojej działalności.

– **Badanie poświęcone zmianie dostawców usług w chmurze**, w ramach którego w drugim kwartale 2017 r. zorganizowano międzysektorowe warsztaty.

– **Badanie służące wsparciu przeglądu dyrektywy w sprawie baz danych** obejmujące rozmowy z określonymi zainteresowanymi stronami. Przeprowadzenie tego badania ułatwiło Komisji przygotowanie oceny skutków na potrzeby przeglądu dyrektywy w sprawie baz danych przeprowadzanego w kontekście aktu w sprawie danych oraz osiągnięcie wspólnych celów tych dwóch aktów prawnych.

– **Wsparcie metodologiczne udzielone na potrzeby oceny skutków związanych z wykorzystywaniem danych będących w posiadaniu podmiotów prywatnych do celów statystyki publicznej**. Przedmiotowe działanie dostarczyło danych wejściowych na potrzeby oceny wpływu zjawiska ponownego wykorzystywania danych do celów statystyki publicznej w relacjach między przedsiębiorstwami a administracją publiczną poprzez opracowanie podejścia metodologicznego i opisanie korzyści i kosztów związanych z ponownym wykorzystywaniem danych, a także omówienie wybranych przypadków użycia dotyczących różnych dziedzin statystycznych i różnych rodzajów danych gromadzonych przez podmioty sektora prywatnego. Ponadto działanie to wnosi wkład w trwające badania i dyskusje i przyczynia się do lepszego zrozumienia zjawiska wymiany danych między przedsiębiorstwami a organami administracji.

– **Seminaria internetowe dotyczące platform danych osobowych i platform danych przemysłowych**. 6, 7 i 8 maja 2020 r. zorganizowano trzy seminaria internetowe. Wzięli w nich udział przedstawiciele stosownych projektów dotyczących platform danych wchodzących w skład portfela projektów partnerstwa publiczno-prywatnego na rzecz dużych zbiorów danych.

– **Grupa Ekspertów Wysokiego Szczebla ds. Wymiany Danych Między Przedsiębiorstwami a Organami Administracji.** W sprawozdaniu sporządzonym przez tę grupę przedstawiono wyniki analizy problemów związanych z wymianą danych między przedsiębiorstwami a organami administracji w Unii i zaproponowano zbiór zaleceń służących zapewnieniu skalowalnej, odpowiedzialnej i zrównoważonej wymiany danych między przedsiębiorstwami a organami administracji w interesie publicznym. Oprócz zalecenia dla Komisji, by zbadała możliwość wprowadzenia ram prawnych w tej dziedzinie, w sprawozdaniu przedstawiono kilka sposobów zachęcania prywatnych przedsiębiorstw do udostępniania ich danych. Obejmują one zachęty pieniężne i niepieniężne, np.

bodźce podatkowe, inwestowanie funduszy publicznych w celu wspierania rozwoju zaufanych narzędzi technicznych i systemów uznawania na potrzeby udostępniania danych.

– **Warsztaty dotyczące oznakowań dla dostawców rozwiązań technicznych w zakresie wymiany danych/certyfikacji takich dostawców**. W seminarium internetowym poświęconym tej problematyce, które odbyło się 12 maja 2020 r., wzięło udział około stu uczestników reprezentujących przedsiębiorstwa (w tym MŚP), instytucje europejskie i środowisko akademickie. Celem tego seminarium było zbadanie, czy wprowadzenie systemu oznakowania lub certyfikacji mogłoby przyspieszyć tempo wprowadzania przez przedsiębiorstwa rozwiązań związanych z pośrednikami w zakresie danych poprzez zwiększenie poziomu zaufania do ekosystemu danych.

– **W dziesięciu warsztatach zorganizowanych w okresie od lipca do listopada 2019 r. wzięło udział ponad 300 zainteresowanych stron z różnych sektorów**. W trakcie warsztatów omówiono, w jaki sposób uporządkowanie procesu **udostępniania danych w niektórych dziedzinach** takich jak środowisko, rolnictwo, energetyka lub opieka zdrowotna mogłoby okazać się korzystne dla społeczeństwa rozumianego jako całość, wspierając podmioty publiczne w opracowywaniu lepszych polityk i udoskonalaniu usług publicznych, a także ułatwiając podmiotom prywatnym świadczenie usług wnoszących wkład w przezwyciężanie wyzwań społecznych.

– **Konsultacje w ramach panelu MŚP.** Przedmiotowe konsultacje, które były prowadzone w okresie od października 2018 r. do stycznia 2019 r., miały na celu zasięgnięcie opinii MŚP w kwestii opracowanych przez Komisję zasad dotyczących udostępniania danych między przedsiębiorstwami oraz wytycznych opublikowanych w komunikacie pt. „W kierunku wspólnej europejskiej przestrzeni danych” oraz w towarzyszącym mu dokumencie roboczym służb Komisji z 25 kwietnia 2018 r.[51]

– **Najnowsze badanie Eurobarometru dotyczące skutków cyfryzacji.** W tej ogólnej ankiecie poświęconej codziennemu życiu Europejczyków zawarto pytania dotyczące kontroli obywateli nad ich danymi osobowymi oraz udostępniania przez nich tych danych. Wyniki badania, które opublikowano 5 marca 2020 r., dostarczają informacji na temat gotowości obywateli Unii do udostępniania ich danych osobowych, a także warunków, na jakich są oni gotowi udostępniać takie dane.

– **Opinia Europejskiego Inspektora Ochrony Danych** (EIOD) w sprawie europejskiej strategii w zakresie danych[52]. 16 czerwca 2020 r. EIOD przyjął opinię nr 3/2020 w sprawie europejskiej strategii w zakresie danych. EIOD z zadowoleniem odnotował opracowanie tej strategii i uznał, że jej wdrożenie będzie dobrą okazją do zaprezentowania przykładu alternatywnego modelu gospodarki opartej o dane.

• **Ocena skutków**

Niniejszemu wnioskowi towarzyszy ocena skutków[53], która została przedłożona Radzie ds. Kontroli Regulacyjnej 29 września 2021 r. i 13 grudnia 2021 r. W dniu 21 stycznia 2022 r. Rada wydała opinię pozytywną z zastrzeżeniami.

---

51 COM(2018) 232 final; SWD(2018) 125 final z 25.4.2018.

52 Opinia EIOD nr 3/2020 w sprawie europejskiej strategii w zakresie danych.

53 **[Należy wstawić linki do ostatecznej wersji dokumentu oraz do streszczenia.]**

- **Sprawność regulacyjna i uproszczenie**

Poprzez wyjaśnienie, że prawo *sui generis*, o którym mowa w dyrektywie w sprawie baz danych (dyrektywa 96/9/WE), nie ma zastosowania do baz danych zawierających dane wygenerowane lub pozyskane wskutek korzystania z produktów lub powiązanych usług, wniosek gwarantuje, że prawo *sui generis* nie będzie kolidowało z prawami przedsiębiorstw i konsumentów dotyczącymi dostępu do danych, korzystania z danych i ich udostępniania przewidzianymi w przedmiotowym rozporządzeniu. Wspomniane wyjaśnienie doprowadzi do dostosowania sposobu korzystania z prawa *sui generis* do celu przedmiotowego wniosku ustawodawczego, przyczyni się do zapewnienia jednolitego stosowania przepisów na rynku wewnętrznym i wniesie wkład w budowę gospodarki opartej o dane.

Dzięki ułatwieniu możliwości uzyskania dostępu do danych i ich wykorzystywania akt w sprawie danych powinien doprowadzić do zmniejszenia obciążeń zarówno dla podmiotów sektora publicznego, jak i dla przedsiębiorstw, głównie dzięki obniżeniu kosztów transakcyjnych i generowaniu przyrostów wydajności. Zgodnie z zasadą „jedno więcej – jedno mniej”[54], której celem jest ograniczanie do minimum nakładanych na obywateli i przedsiębiorstwa obciążeń związanych ze skutkami i kosztami stosowania przepisów, szacunkowe obciążenia administracyjne netto związane z aktem w sprawie danych określone na podstawie wyników oceny skutków przełożą się na korzyści, które prawdopodobnie nie tylko zrównoważą powiązane koszty administracyjne, ale będą nad nimi zdecydowanie przeważały.

- **Prawa podstawowe**

Wniosek jest zgodny z przepisami Unii dotyczącymi ochrony danych osobowych i prywatności komunikacji oraz urządzeń końcowych; przewidziano w nim dodatkowe środki zabezpieczające w kwestiach dotyczących dostępu do danych osobowych, a także w przypadkach regulowanych przepisami dotyczącymi praw własności intelektualnej.

W rozdziale II wysoki poziom ochrony konsumentów został dodatkowo wzmocniony w rezultacie ustanowienia nowego prawa dostępu do danych wygenerowanych przez użytkownika w sytuacjach, które nie podlegały wcześniej przepisom prawa Unii. Prawo do rozporządzania majątkiem uzyskanym zgodnie z prawem i zbywania tego majątku zostało wzmocnione dzięki ustanowieniu prawa dostępu do danych wygenerowanych wskutek korzystania z przedmiotów związanych z internetem rzeczy. Dzięki temu właściciel rzeczy może cieszyć się lepszym doświadczeniem użytkownika i uzyskać dostęp do szerszego spektrum usług, np. usług naprawy i usług konserwacyjnych. Jeżeli chodzi o ochronę konsumentów, prawa dzieci jako konsumentów podatnych na zagrożenia zasługują na szczególną uwagę, przy czym przepisy aktu w sprawie danych przyczynią się do zapewnienia większej przejrzystości w kwestii dostępu do danych i przypadków użycia.

Przysługujące osobom trzecim prawo do uzyskania dostępu do danych w ramach internetu rzeczy na wniosek użytkownika ogranicza wolność prowadzenia działalności gospodarczej i swobodę zawierania umów producenta lub twórcy produktu lub powiązanej usługi. Ograniczenie to należy uznać za uzasadnione, ponieważ przyczynia się ono do poprawy ochrony konsumentów, a w szczególności sprzyja propagowaniu interesów ekonomicznych konsumenta. Producent lub twórca produktu lub powiązanej usługi dysponuje zazwyczaj wyłączną kontrolą nad sposobem korzystania z danych generowanych wskutek użytkowania produktu lub powiązanej usługi, co prowadzi do blokad technologicznych i utrudnia wejście na rynek podmiotom oferującym usługi na rynkach niższego szczebla. Prawo dostępu do

[54] SWD(2021) 305 final.

danych w ramach internetu rzeczy odnosi się do tej sytuacji poprzez dodatkowe wzmocnienie pozycji konsumentów korzystających z produktów lub powiązanych usług, zapewniając im możliwość rzeczywistego kontrolowania sposobu wykorzystywania danych generowanych w rezultacie korzystania przez nich z danego produktu lub powiązanej z nim usługi oraz stwarzając warunki sprzyjające innowacyjności ze strony większej liczby podmiotów działających na rynku. Dzięki wprowadzeniu tego prawa konsumenci będą dysponowali szerszym wyborem usług na rynkach niższego szczebla, takich jak usługi naprawy i konserwacji, i nie będą już uzależnieni wyłącznie od usług świadczonych przez producenta. Wniosek ułatwia przekazywanie danych użytkownika osobom trzecim, zapewniając tym samym możliwość świadczenia konkurencyjnych usług na rynkach niższego szczebla, a także zwiększając potencjał w zakresie innowacyjności opartej na danych oraz opracowywania produktów lub usług niepowiązanych z produktami lub usługami pierwotnie zakupionymi przez użytkownika lub produktami lub usługami, na korzystanie z których użytkownik pierwotnie wykupił abonament.

Ograniczenie swobody zawierania umów i wolności prowadzenia działalności gospodarczej producenta lub twórcy należy uznać za proporcjonalne i zrównoważone faktem, że producent lub projektant również może korzystać z danych, o ile robi to zgodnie z obowiązującymi przepisami i w porozumieniu z użytkownikiem. Ponadto producent lub twórca będzie również czerpał korzyści z tytułu przysługującego mu prawa do zażądania wynagrodzenia za zapewnienie osobie trzeciej dostępu do danych. Takie prawo dostępu pozostaje bez uszczerbku dla istniejących praw dostępu do danych i praw do przenoszenia danych przysługujących osobom, których dane dotyczą, zgodnie z przepisami RODO. Dodatkowe środki zabezpieczające zapewniają proporcjonalne wykorzystywanie danych przez osobę trzecią.

Na mocy przepisów zawartych w rozdziale IV ustanowiono sprawiedliwy i skuteczny system ochrony przed nieuczciwymi postanowieniami umownymi w dziedzinie udostępniania danych, który przyczyni się do zwiększenia zdolności mikroprzedsiębiorstw oraz małych lub średnich przedsiębiorstw do prowadzenia działalności gospodarczej. Przepisy te ograniczają swobodę zawierania umów przysługującą przedsiębiorstwom objętych ich zakresem tylko w pewnym zakresie, ponieważ odnoszą się wyłącznie do nieuczciwych postanowień umownych dotyczących dostępu do danych i korzystania z danych jednostronnie narzucanych przez jedną stronę umowy na mikroprzedsiębiorstwo lub na małe lub średnie przedsiębiorstwo. Wprowadzenie tych przepisów należy uznać za uzasadnione, ponieważ MŚP znajdują się zazwyczaj w słabszej pozycji negocjacyjnej i niejednokrotnie nie mają innego wyjścia niż zaakceptowanie postanowień umownych oferowanych na zasadzie „przyjmij albo zrezygnuj”. Swoboda zawierania umów pozostaje w dużej mierze nieograniczona, ponieważ nie dopuszcza się wyłącznie zawierania umów na nieproporcjonalnych i nieuczciwych warunkach, a już zawarte umowy w miarę możliwości pozostają w mocy po usunięciu z nich nieuczciwych postanowień umownych. Ponadto strony nadal mogą prowadzić indywidualne negocjacje dotyczące konkretnego postanowienia umownego[55].

Przepisy dotyczące wymiany danych między przedsiębiorstwami a organami administracji w przypadku wystąpienia wyjątkowej potrzeby zawarte w rozdziale V zwiększą zdolność organów publicznych do podejmowania działań leżących we wspólnym interesie takich jak działania podejmowane w reakcji na niebezpieczeństwo publiczne, działania służące zapobieżeniu niebezpieczeństwu publicznemu lub działania wspierające przywracanie stanu

[55] Aby zapoznać się z dodatkowymi informacjami na temat analizy nieuczciwego charakteru i zasady swobody zawierania umów, zob. załącznik 11 do oceny skutków.

wyjściowego po wystąpieniu niebezpieczeństwa publicznego. Uproszczenie procedur zwracania się z wnioskiem o udostępnienie danych przyniesie również korzyści podmiotom z sektora prywatnego.

Przepisy dotyczące zmiany dostawców usług przetwarzania danych zawarte w rozdziale VI wzmacniają pozycję klientów będących podmiotami gospodarczymi i gwarantują im możliwość zmiany dostawcy tych usług. Ograniczenie prawa dostawców usług przetwarzania danych do prowadzenia działalności gospodarczej jest uzasadnione, ponieważ nowe przepisy mają na celu usunięcie blokad technologicznych na rynku przetwarzania w chmurze i przetwarzania brzegowego oraz zapewnienie użytkownikom będącym podmiotami gospodarczymi oraz osobom fizycznym możliwości wyboru dostawcy usług przetwarzania danych.

Przewidziana w rozdziale X interwencja dotycząca ustanowionego w dyrektywie w sprawie baz danych prawa *sui generis* przysługującego producentowi bazy danych nie ogranicza ochrony praw własności intelektualnej zapewnianej na mocy tej dyrektywy. Przeciwnie, interwencja ta zwiększa pewność prawa w przypadkach, w których kwestie związane z ochroną wynikającą z prawa *sui generis* pozostały wcześniej niejasne.

4. WPŁYW NA BUDŻET

Niniejszy wniosek nie będzie miał żadnego wpływu na budżet.

5. ELEMENTY FAKULTATYWNE

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

Na poziomie sektorowym i makroekonomicznym prowadzone obecnie badanie służące monitorowaniu sytuacji na rynku danych ułatwi prześledzenie wpływu gospodarczego przedmiotowego wniosku na rynek danych w Unii.

Wpływ nowych przepisów na MŚP, w szczególności jeżeli chodzi o sposób, w jaki postrzegają one problemy związane z dostępem do danych i korzystaniem z danych, zostanie oceniony w trakcie konsultacji w ramach panelu MŚP zorganizowanych po upływie pięciu lat od dnia przyjęcia aktu w sprawie danych.

Biorąc pod uwagę centralną rolę wspólnych europejskich przestrzeni danych w procesie wdrażania europejskiej strategii w zakresie danych, wiele skutków tej inicjatywy będzie monitorowane na poziomie sektorowych przestrzeni danych w oparciu o dane gromadzone przez Centrum Wsparcia Przestrzeni Danych, które ma być finansowane w ramach programu „Cyfrowa Europa”. Regularna współpraca między służbami Komisji, Centrum Wsparcia i Europejską Radą ds. Innowacji w zakresie Danych (która ma zostać ustanowiona po wejściu w życie aktu w sprawie zarządzania danymi) powinna stanowić wiarygodne źródło informacji pozwalających ocenić postępy w tym obszarze.

Ponadto po upływie czterech lat od przyjęcia aktu w sprawie danych planuje się przeprowadzenie oceny inicjatywy i – w razie potrzeby – przygotowanie dalszych działań.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

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

Przepisy zawarte w rozdziale II zwiększają pewność prawa dla konsumentów i przedsiębiorstw w zakresie uzyskiwania dostępu do danych wygenerowanych przez produkty lub powiązane usługi, których są oni właścicielami, które wynajmują lub z których korzystają na zasadzie leasingu. Producenci i twórcy muszą opracowywać swoje produkty w taki sposób, aby wyjściowo zapewnić możliwość łatwego uzyskania dostępu do danych; będą oni również zobowiązani do zagwarantowania przejrzystości w kwestii tego, które dane zostaną udostępnione i w jaki sposób będzie można uzyskać do nich dostęp. Przepisy zawarte w tym rozdziale nie uniemożliwią producentom uzyskiwania dostępu do danych generowanych przez oferowane przez nich produkty lub powiązane usługi i korzystania z takich danych, o ile uzyskają oni na to zgodę użytkownika. Posiadacz danych będzie zobowiązany udostępnić tego rodzaju dane osobom trzecim na wniosek użytkownika. Użytkownicy będą uprawnieni do upoważnienia posiadacza danych do udostępnienia danych dostawcom usług będącym osobami trzecimi takim jak dostawcy usług na rynkach niższego szczebla. Powyższe zobowiązania nie będą miały zastosowania do mikroprzedsiębiorstw i małych przedsiębiorstw.

W rozdziale III przedstawiono przepisy ogólne mające zastosowanie do obowiązków w zakresie udostępniania danych. W przypadku gdy posiadacz danych jest zobowiązany udostępnić dane odbiorcy danych zgodnie z przepisami rozdziału II lub innymi przepisami prawa Unii lub ustawodawstwem państwa członkowskiego, ramy ogólne będą określały warunki, na których takie dane powinny zostać udostępnione, a także wysokość wynagrodzenia z tytułu ich udostępnienia. Wszelkie takie warunki będą musiały być sprawiedliwe i niedyskryminacyjne, a wszelkie wynagrodzenie będzie musiało zostać ustalone na rozsądnym poziomie, przy czym inne przepisy prawa Unii lub ustawodawstwa krajowego wdrażającego prawo Unii będą mogły uchylić konieczność wypłaty wynagrodzenia z tytułu udostępnienia danych lub obniżyć kwotę takiego wynagrodzenia. Kwota jakiegokolwiek wynagrodzenia żądanego od MŚP nie może przewyższać kosztów poniesionych w związku z koniecznością udostępnienia danych, chyba że przepisy obowiązujące w danym sektorze stanowią inaczej. Organy zajmujące się rozstrzyganiem sporów certyfikowane przez państwa członkowskie mogą udzielać wsparcia stronom, które nie są w stanie osiągnąć porozumienia w kwestii wysokości wynagrodzenia z tytułu udostępnienia danych lub warunków, na których dane są udostępniane.

W rozdziale IV odniesiono się do kwestii nieuczciwego charakteru postanowień umownych w umowach dotyczących udostępniania danych zawieranych między przedsiębiorstwami w sytuacjach, w których jedna ze stron jednostronnie narzuca dane postanowienie umowne mikroprzedsiębiorstwu albo małemu lub średniemu przedsiębiorstwu. Przepisy zawarte w tym rozdziale gwarantują, że porozumienia umowne dotyczące udostępniania danych i korzystania z danych nie będą wykorzystywały braku równowagi pod względem pozycji negocjacyjnej stron umowy. W przepisach dotyczących instrumentu analizy nieuczciwego charakteru przewidziano przepis ogólny ustanawiający definicję nieuczciwego charakteru postanowienia umownego związanego z udostępnianiem danych; definicję tę uzupełnia wykaz postanowień, które zawsze uznaje się za nieuczciwe albo w odniesieniu do których przyjmuje się domniemanie ich nieuczciwości. W przypadku braku równowagi pod względem pozycji negocjacyjnej analiza chroni słabszą stronę umowy, co pozwala zapobiec zawieraniu nieuczciwych umów. Nieuczciwy charakter postanowień umownych utrudnia obydwu stronom umowy korzystanie z danych. Dzięki wprowadzeniu analizy nieuczciwego charakteru przepisy rozporządzenia zapewniają możliwość sprawiedliwszego podziału

wartości w gospodarce opartej o dane[56]. Modelowe postanowienia umowne rekomendowane przez Komisję mogą ułatwić stronom będącym podmiotami komercyjnymi zawieranie umów na uczciwych warunkach.

W rozdziale V ustanowiono zharmonizowane ramy regulujące kwestie związane z korzystaniem przez organy sektora publicznego oraz instytucje, agencje i organu Unii z danych znajdujących się w posiadaniu przedsiębiorstw w przypadku wystąpienia wyjątkowej potrzeby uzyskania dostępu do danych będących przedmiotem wniosku. Ramy te opierają się na obowiązku udostępniania danych i byłyby wykorzystywane wyłącznie w przypadku wystąpienia niebezpieczeństwa publicznego lub w sytuacjach, w których organy sektora publicznego uznają, że zaistniała wyjątkowa potrzeba skorzystania z określonych danych, przy czym danych tych nie sposób jest pozyskać na rynku, w odpowiednim terminie poprzez przyjęcie nowych przepisów ani przy wykorzystaniu już istniejących obowiązków sprawozdawczych. W przypadku zaistnienia wyjątkowej potrzeby podjęcia działań w związku z niebezpieczeństwem publicznym takim jak stan zagrożenia zdrowia publicznego lub poważna klęska żywiołowa bądź poważna katastrofa spowodowana przez człowieka dane byłyby udostępniane nieodpłatnie. W innych przypadkach, w których doszło do wystąpienia wyjątkowej potrzeby, uwzględniając sytuację służącą zapobieżeniu niebezpieczeństwu publicznemu lub wniesieniu wkładu w przywracanie stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego, posiadacz danych udostępniający dane powinien być upoważniony do otrzymania wynagrodzenia w kwocie odpowiadającej kosztom związanym z udostępnieniem stosownych danych powiększonej o rozsądnej wysokości marżę. Aby zagwarantować, że prawo do wystąpienia z wnioskiem o udostępnienie danych nie będzie nadużywane i że podmioty sektora publicznego pozostaną odpowiedzialne za sposób korzystania z tego prawa, wnioski o udostępnienie danych będą musiały być proporcjonalne, precyzyjnie wskazywać cel, w jakim dane mają zostać wykorzystane, oraz zapewniać poszanowanie interesów przedsiębiorstwa udostępniającego dane. Właściwe organy dbałyby o przejrzystość wszystkich wniosków oraz ich publiczną dostępność. Byłyby również odpowiedzialne za rozpatrywanie wszelkich powiązanych z nimi skarg.

W rozdziale VI wprowadzono minimalne wymogi regulacyjne o charakterze umownym, komercyjnym i technicznym nakładane na dostawców usług w chmurze, usług przetwarzania brzegowego i innych usług przetwarzania danych, aby umożliwić użytkownikom zamianę takich usług. W szczególności we wniosku zawarto przepisy gwarantujące klientom zachowanie równoważności funkcjonalnej (minimalnego poziomu funkcjonalności) usługi po zmianie dostawcy usług. We wniosku przewidziano możliwość zastosowania odstępstwa od wymogu równoważności z uwagi na brak możliwości technicznych, ale w takim wypadku ciężar dowodu spoczywa na dostawcy usług. We wniosku nie wprowadzono nakazu korzystania z określonych standardów technicznych ani interfejsów. Usługi muszą być jednak świadczone zgodnie z normami europejskimi lub – w stosownych przypadkach – z otwartymi specyfikacjami technicznymi w zakresie interoperacyjności.

W rozdziale VII odniesiono się do kwestii bezprawnego dostępu osoby trzeciej do danych nieosobowych przechowywanych w Unii za pośrednictwem usług przetwarzania danych oferowanych na rynku unijnym. Przedmiotowy wniosek nie wywiera wpływu na podstawę prawną wniosków o udostępnienie danych odnoszących się do danych znajdujących się w posiadaniu obywateli Unii lub przedsiębiorstw unijnych i pozostaje bez uszczerbku dla unijnych ram ochrony danych i prywatności. Przewidziano w nim konkretne środki zabezpieczające, m.in. zobowiązanie dostawców usług do podejmowania wszelkich

[56] Aby zapoznać się z dodatkowymi informacjami na temat analizy nieuczciwego charakteru oraz jej stosowania w praktyce, zob. załącznik 11 do oceny skutków.

uzasadnionych działań o charakterze technicznym, prawnym i organizacyjnym, aby nie dopuścić do przypadku zapewnienia dostępu do danych, jeżeli udostępnienie danych byłoby sprzeczne z przewidzianymi w prawie Unii zobowiązaniami w zakresie ochrony takich danych, chyba że w danej sytuacji spełniono rygorystyczne warunki. Rozporządzenie jest zgodne z zobowiązaniami międzynarodowymi zaciągniętymi przez Unię wobec WTO i z postanowieniami dwustronnych umów handlowych.

W rozdziale VIII ustanowiono zasadnicze wymagania w zakresie interoperacyjności, których operatorzy przestrzeni danych i dostawcy usług przetwarzania danych są zobowiązani przestrzegać, jak również zasadnicze wymagania dotyczące inteligentnych umów. W rozdziale tym zapewniono również możliwość stosowania otwartych specyfikacji w zakresie interoperacyjności i norm europejskich w kwestiach związanych z interoperacyjnością usług w zakresie przetwarzania danych, aby wspierać budowanie sprawnie funkcjonującego środowiska chmury obliczeniowej bazującego na usługach świadczonych przez wielu dostawców.

W rozdziale IX ustanowiono ramy wdrażania i egzekwowania przepisów, które będą stosowane we współpracy z właściwymi organami w poszczególnych państwach członkowskich i które obejmują również mechanizm rozpatrywania skarg. Komisja przedstawi zalecenia w zakresie dobrowolnych modelowych postanowień umownych w umowach dotyczących dostępu do danych i wykorzystywania danych. Naruszenie przepisów przedmiotowego rozporządzenia będzie podlegało karze.

W rozdziale X zawarto przepis mający na celu zagwarantowanie, aby prawo *sui generis* przewidziane w dyrektywie 96/9/WE nie miało zastosowania do baz danych zawierających dane pozyskane lub wygenerowane podczas korzystania z produktu lub powiązanej usługi, uniemożliwiając tym samym ograniczanie skutecznego wykonywania prawa dostępu do danych i korzystania z danych przysługującego użytkownikom zgodnie z art. 4 przedmiotowego rozporządzenia lub prawa do udostępniania takich danych osobom trzecim zgodnie z art. 5 tego rozporządzenia.

W rozdziale XI Komisję upoważniono do przyjmowania aktów delegowanych służących wprowadzeniu mechanizmu monitorowania opłat z tytułu zamiany nakładanych na dostawców usług przetwarzania danych, doprecyzowaniu kluczowych wymogów w zakresie interoperacyjności i opublikowaniu odniesienia do otwartych specyfikacji w zakresie interoperacyjności i norm europejskich dotyczących interoperacyjności usług przetwarzania danych. W rozdziale tym przewidziano również procedurę komitetową na potrzeby przyjmowania aktów wykonawczych, aby usprawnić proces przyjmowania wspólnych specyfikacji w zakresie interoperacyjności i inteligentnych umów w przypadkach, w których nie opracowano norm zharmonizowanych lub takie normy są niewystarczające do zapewnienia zgodności z zasadniczymi wymaganiami. We wniosku wyjaśniono również pozycję rozporządzenia względem innych aktów prawnych Unii regulujących kwestie związane z prawami i obowiązkami w zakresie udostępniania danych.

2022/0047 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (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 Komitetu Ekonomiczno-Społecznego[57],

uwzględniając opinię Komitetu Regionów[58],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

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 rzeczy 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. Ten sam zbiór danych może zostać potencjalnie wykorzystany i ponownie wykorzystany do wielu różnych celów i w nieograniczonym zakresie, bez jakiegokolwiek uszczerbku dla jakości czy ilości znajdujących się w nim danych.

(2) Bariery utrudniające udostępnianie danych uniemożliwiają optymalne wykorzystywanie danych z korzyścią dla całego społeczeństwa. Wspomniane bariery obejmują brak czynników zachęcających posiadaczy danych do dobrowolnego zawierania umów o udostępnianie danych, brak pewności w kwestii praw i obowiązków w zakresie danych, koszty przeprowadzania zamówień na interfejsy techniczne i wdrażania tych interfejsów, wysoki poziom rozdrobnienia informacji w silosach danych, niezadowalającą jakość zarządzania metadanymi, brak norm w zakresie interoperacyjności semantycznej i technicznej, wąskie gardła utrudniające uzyskanie dostępu do danych, brak wspólnych praktyk w dziedzinie udostępniania danych oraz nadużywanie braku równowagi kontraktowej w kwestiach dotyczących dostępu do danych i ich wykorzystywania.

---

57 Dz.U. C […] z […], s. […].

58 Dz.U. C […] z […], s. […].

(3) W sektorach charakteryzujących się znacznym udziałem mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw można niejednokrotnie zaobserwować niedobór zdolności cyfrowych oraz umiejętności gromadzenia, analizowania i wykorzystywania danych; ponadto w takich sektorach dostęp do danych jest często ograniczony z uwagi na fakt, że jeden podmiot przechowuje je w swoim systemie lub z uwagi na brak interoperacyjności między danymi, brak interoperacyjności między usługami w zakresie danych lub brak interoperacyjności transgranicznej.

(4) Aby zaspokoić potrzeby gospodarki cyfrowej i usunąć bariery stojące na drodze dobrze prosperującego wewnętrznego rynku danych, należy ustanowić zharmonizowane ramy określające, kto poza producentem lub innym posiadaczem danych jest uprawniony do uzyskania dostępu do danych generowanych przez produkty lub powiązane usługi, na jakich warunkach i na jakiej podstawie. Dlatego też państwa członkowskie nie powinny przyjmować ani utrzymywać dodatkowych wymogów krajowych odnoszących się do kwestii wchodzących w zakres niniejszego rozporządzenia, chyba że niniejsze rozporządzenie wyraźnie stanowi inaczej, ponieważ taka sytuacja wywarłaby wpływ na możliwość bezpośredniego i jednolitego stosowania przepisów niniejszego rozporządzenia.

(5) Celem niniejszego rozporządzenia jest zapewnienie użytkownikom produktu lub powiązanej usługi w Unii możliwości terminowego uzyskania dostępu do danych generowanych w rezultacie korzystania z danego produktu lub powiązanej usługi oraz wykorzystywania tych danych, jak również udostępniania ich wybranym przez siebie osobom trzecim. Zgodnie z przepisami niniejszego rozporządzenia posiadacz danych jest w określonych okolicznościach zobowiązany do udostępnienia danych użytkownikom i osobom trzecim wskazanym przez użytkowników. Niniejsze rozporządzenie gwarantuje również, że posiadacze danych będą udostępniali dane odbiorcom danych w Unii na sprawiedliwych, rozsądnych i niedyskryminujących warunkach oraz w przejrzysty sposób. Przepisy prawa prywatnego mają kluczowe znaczenie w ogólnie rozumianych ramach udostępniania danych. Z tego względu w niniejszym rozporządzeniu dostosowuje się przepisy prawa zobowiązań i dąży się do zapobiegania wykorzystywaniu braku równowagi kontraktowej, ponieważ zjawisko to utrudnia mikroprzedsiębiorstwom oraz małym lub średnim przedsiębiorstwom w rozumieniu zalecenia 2003/361/WE możliwość uzyskiwania dostępu do danych i wykorzystywania danych na uczciwych warunkach. Niniejsze rozporządzenie nakłada również na posiadaczy danych obowiązek udostępniania organom sektora publicznego państw członkowskich oraz instytucjom, agencjom lub podmiotom unijnym – w przypadku wystąpienia wyjątkowej potrzeby – danych niezbędnych do wykonywania zadań leżących w interesie publicznym. Celem niniejszego rozporządzenia jest ponadto ułatwienie przechodzenia z jednych na drugie usługi w zakresie przetwarzania danych oraz zwiększenie interoperacyjności danych oraz mechanizmów i usług w zakresie udostępniania danych w Unii. Przepisów niniejszego rozporządzenia nie należy interpretować jako uznających ani tworzących jakąkolwiek podstawę prawną upoważniającą posiadacza danych do przechowywania danych, uzyskiwania do nich dostępu lub ich przetwarzania ani jako przyznających posiadaczowi danych jakiekolwiek nowe prawo do wykorzystywania danych generowanych w wyniku korzystania z produktu lub powiązanej usługi. W rozporządzeniu przyjmuje się natomiast jako punkt wyjścia poziom kontroli, jaki rzeczywiście przysługuje posiadaczowi danych – *de facto* lub *de iure* – względem danych generowanych przez produkty lub powiązane usługi.

(6) Generowanie danych stanowi rezultat działań co najmniej dwóch podmiotów – twórcy lub producenta produktu i użytkownika tego produktu. Ta sytuacja otwiera debatę dotyczącą sprawiedliwości w gospodarce cyfrowej, ponieważ dane rejestrowane przez takie produkty lub powiązane usługi stanowią istotne dane wejściowe dla usług świadczonych na rynkach niższego szczebla, usług pomocniczych oraz innego rodzaju usług. Aby zapewnić możliwość czerpania znacznych korzyści ekonomicznych, jakie dane rozumiane jako dobro nierywalizacyjne mogą przynieść dla gospodarki i społeczeństwa, należy przyjąć ogólne podejście regulujące kwestie związane z udzielaniem praw dostępu do danych i korzystania z danych zamiast przyznawania wyłącznych praw w zakresie dostępu do danych i ich wykorzystywania.

(7) Podstawowe prawo do ochrony danych osobowych zostało zagwarantowane w szczególności w rozporządzeniu (UE) 2016/679 i rozporządzeniu (UE) 2018/1725. W dyrektywie 2002/58/WE zapewniono dodatkową ochronę życia prywatnego i poufności komunikacji, a także określono warunki przechowywania wszelkich danych osobowych i nieosobowych w urządzeniach końcowych oraz warunki uzyskiwania dostępu do tych danych z poziomu urządzeń końcowych. Wspomniane instrumenty prawne zapewniają podstawę dla zrównoważonego i odpowiedzialnego przetwarzania danych, również w sytuacjach, w których zbiory danych uwzględniają połączenie danych osobowych z danymi nieosobowymi. Niniejsze rozporządzenie uzupełnia prawo Unii w zakresie ochrony danych i prywatności, w szczególności rozporządzenie (UE) 2016/679 i 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.

(8) Zasady minimalizacji danych, ochrony danych w fazie projektowania i 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 udostępniania danych, w tym również strony podlegające przepisom niniejszego rozporządzenia, powinny wdrażać środki techniczne i organizacyjne przyczyniające się do zapewnienia ochrony tych praw. Takie środki obejmują nie tylko pseudonimizację i szyfrowanie, ale również korzystanie z coraz powszechniej dostępnej technologii umożliwiającej wkomponowywanie algorytmów w dane, co pozwala uzyskać wartościowe informacje bez konieczności przesyłania danych między stronami lub zbędnego kopiowania samych surowych lub ustrukturyzowanych danych.

(9) Niniejsze rozporządzenie uzupełnia prawo Unii służące wspieraniu interesów konsumentów i zapewnieniu wysokiego poziomu ochrony konsumentów, ochrony zdrowia konsumentów, ich bezpieczeństwa oraz ich interesów gospodarczych, w szczególności dyrektywę 2005/29/WE Parlamentu Europejskiego i Rady[59], dyrektywę Parlamentu Europejskiego i Rady 2011/83/UE[60] oraz dyrektywę Rady 93/13/EWG[61], i pozostaje bez uszczerbku dla tego prawa.

---

[59] 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).

[60] 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

(10) Niniejsze rozporządzenie pozostaje bez uszczerbku dla aktów prawnych Unii regulujących kwestie związane z udostępnianiem danych, uzyskiwaniem do nich dostępu oraz ich wykorzystywaniem do celów związanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem lub ściganiem czynów zabronionych lub wykonywaniem kar lub do celów celnych bądź podatkowych, niezależnie od podstawy prawnej przewidzianej w Traktacie o funkcjonowaniu Unii Europejskiej, w oparciu o którą zostały one przyjęte. Wspomniane akty obejmują rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, [wnioski dotyczące rozporządzenia w sprawie elektronicznego materiału dowodowego [COM(2018) 225 i COM(2018) 226] po ich przyjęciu], [wniosek dotyczący] rozporządzenia Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniającego dyrektywę 2000/31/WE, a także współpracę międzynarodową w tym zakresie prowadzoną w szczególności na podstawie Konwencji Rady Europy z 2001 r. o cyberprzestępczości („Konwencja o cyberprzestępczości"). Niniejsze rozporządzenie pozostaje bez uszczerbku dla kompetencji państw członkowskich w odniesieniu do działań związanych z bezpieczeństwem publicznym, obroną i bezpieczeństwem narodowym zgodnie z prawem Unii oraz działań organów celnych w zakresie zarządzania ryzykiem i ogólnie w zakresie weryfikacji przestrzegania kodeksu celnego przez podmioty gospodarcze.

(11) Niniejsze rozporządzenie nie powinno mieć wpływu na przepisy unijne określające wymogi dotyczące fizycznego projektu i danych w przypadku produktów wprowadzanych do obrotu w Unii.

(12) Niniejsze rozporządzenie stanowi uzupełnienie i nie narusza przepisów unijnych służących określeniu wymogów dostępności niektórych produktów i usług, w szczególności przepisów dyrektywy 2019/882[62].

(13) Niniejsze rozporządzenie pozostaje bez uszczerbku dla kompetencji państw członkowskich w odniesieniu do działań związanych z bezpieczeństwem publicznym, obroną i bezpieczeństwem narodowym zgodnie z prawem Unii oraz działań organów celnych w zakresie zarządzania ryzykiem i ogólnie w zakresie weryfikacji przestrzegania kodeksu celnego przez podmioty gospodarcze.

(14) Zakres stosowania niniejszego rozporządzenia powinien obejmować fizyczne produkty, które pozyskują, generują lub gromadzą, za pomocą swoich elementów składowych, dane dotyczące ich działania, wykorzystania lub środowiska i które mogą przekazywać te dane za pośrednictwem publicznie dostępnych usług łączności elektronicznej (często określane jako internet rzeczy). Do usług łączności elektronicznej należą naziemne sieci telefoniczne, sieci telewizji kablowej, sieci satelitarne i sieci komunikacji zbliżeniowej. Takimi produktami mogą być pojazdy,

---

Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady.

[61] Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2161 z dnia 27 listopada 2019 r. zmieniająca dyrektywę Rady 93/13/EWG i dyrektywy Parlamentu Europejskiego i Rady 98/6/WE, 2005/29/WE oraz 2011/83/UE w odniesieniu do lepszego egzekwowania i unowocześnienia unijnych przepisów dotyczących ochrony konsumenta.

[62] 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).

sprzęty domowe i wyroby konsumpcyjne, wyroby medyczne lub zdrowotne, lub też maszyny rolnicze i przemysłowe. Dane przedstawiają cyfryzację działań i zdarzeń z udziałem użytkowników i w związku z tym użytkownik powinien mieć do nich dostęp, natomiast należy uznać, że informacje uzyskane lub wywnioskowane dzięki tym danym, gdy są posiadane zgodnie z prawem, nie są objęte zakresem stosowania niniejszego rozporządzenia. Takie dane mogą stanowić cenne dane dla użytkowników i przyczyniać się do innowacji i rozwoju usług cyfrowych i innych usług chroniących środowisko, zdrowie i gospodarkę o obiegu zamkniętym, szczególnie poprzez umożliwienie konserwacji i naprawy danych produktów.

(15) Z kolei zakresem stosowania niniejszego rozporządzenia nie powinny być objęte określone produkty, które przede wszystkim służą do wyświetlania lub odtwarzania treści, lub do nagrywania i transmisji treści, przeznaczone między innymi do użytku w ramach usługi online. Do takich produktów należą na przykład komputery osobiste, serwery, tablety i smartfony, kamery, kamery internetowe, systemy do nagrywania dźwięku i skanery tekstu. Takie produkty wymagają udziału człowieka do tworzenia różnego rodzaju form treści, takich jak dokumenty tekstowe, pliki dźwiękowe, pliki wideo, gry, mapy cyfrowe.

(16) Należy określić zasady mające zastosowanie do produktów skomunikowanych obejmujących usługę, bez której nie mogłyby pełnić swojej roli, lub połączonych z taką usługą. Takie powiązane usługi mogą stanowić element umowy sprzedaży, najmu lub leasingu, lub takie usługi są zwykle świadczone w przypadku produktów tego samego rodzaju, w związku z czym użytkownik może spodziewać się świadczenia takich usług ze względu na charakter produktu i biorąc pod uwagę wszelkie publiczne oświadczenia ze strony lub w imieniu sprzedawcy, oddającego w najem, leasingodawcy lub innej osoby na wcześniejszych etapach łańcucha transakcji, w tym producenta. Takie powiązane usługi mogą same generować dane cenne dla użytkownika niezależnie od możliwości gromadzenia danych przez produkt, z którym są połączone. Niniejsze rozporządzenie powinno również mieć zastosowanie do powiązanej usługi dostarczanej nie przez samego sprzedawcę, oddającego w najem lub leasingodawcę, lecz na podstawie umowy sprzedaży, najmu lub leasingu przez osobę trzecią. Jeżeli istnieją wątpliwości w kwestii, czy dostawa usługi stanowi element umowy sprzedaży, najmu lub leasingu, niniejsze rozporządzenie powinno mieć zastosowanie.

(17) Dane generowane w wyniku użytkowania produktu lub powiązanej usługi obejmują dane rejestrowane celowo przez użytkownika. Takie dane obejmują również dane generowane jako produkt uboczny działania użytkownika, w tym dane diagnostyczne, oraz dane generowane bez jakiegokolwiek działania ze strony użytkownika, np. gdy produkt jest w „trybie czuwania", oraz dane rejestrowane w okresach, w których produkt jest wyłączony. Takie dane powinny obejmować dane w formie i formacie, w których zostały wygenerowane przez produkt, ale które nie są związane z danymi wynikającymi z jakiegokolwiek procesu programowego obliczającego dane pochodne tych danych, gdyż taki proces programowy może podlegać prawom własności intelektualnej.

(18) Użytkownika produktu należy rozumieć jako osobę prawną lub fizyczną, w tym przedsiębiorstwo lub konsumenta, która zakupiła albo wzięła w najem lub w leasing dany produkt. W zależności od tytułu prawnego do użytkowania produktu 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 i każdą powiązaną usługę.

(19) W praktyce nie wszystkie dane generowane przez produkt lub powiązane usługi są łatwo dostępne dla użytkowników tego produktu lub powiązanej usługi, a możliwość przenoszenia danych generowanych przez produkty podłączone do internetu rzeczy jest często ograniczona. Użytkownicy nie mogą uzyskać danych potrzebnych do skorzystania z usług naprawy i innych usług oferowanych przez dostawców usług, a przedsiębiorstwa nie mogą wprowadzać innowacyjnych, wydajniejszych i wygodniejszych usług. W wielu sektorach na podstawie kontroli technicznego projektu produktu lub powiązanej usługi producenci często 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 projektowano i wytwarzano, a powiązane usługi świadczono w taki sposób, aby użytkownik zawsze mógł z łatwością uzyskać dostęp do danych generowanych w wyniku użytkowania takich produktów i usług.

(20) Jeżeli kilka osób lub jednostek jest właścicielami danego produktu lub stroną umowy leasingu lub najmu i ma dostęp do powiązanej usługi, przy projektowaniu danego produktu, powiązanej usługi lub stosowanego interfejsu należy dołożyć uzasadnionych starań, aby wszystkie te osoby mogły uzyskać dostęp do generowanych przez nie danych. Użytkownicy produktów generujących dane zwykle muszą założyć konto użytkownika. W ten sposób producent może zidentyfikować użytkownika, a także jest to sposób komunikacji umożliwiający wykonanie i przetwarzanie wniosków o dostęp do danych. Producenci lub projektanci produktu, który zwykle jest wykorzystywany przez kilka osób, powinni zapewnić konieczny mechanizm umożliwiający w razie potrzeby założenie oddzielnych kont użytkownika dla poszczególnych osób lub korzystanie z tego samego konta użytkownika przez kilka osób. Użytkownik powinien uzyskać dostęp za pomocą zwykłego mechanizmu automatycznie wykonującego wniosek bez konieczności analizy lub zatwierdzenia ze strony producenta lub posiadacza danych. Oznacza to, że dane powinny być udostępniane wyłącznie na faktyczne życzenie użytkownika. Jeżeli automatyczne wykonanie wniosku o uzyskanie dostępu do danych jest niemożliwe za pomocą na przykład konta użytkownika lub aplikacji mobilnej zapewnionej wraz z produktem lub usługą, producent powinien poinformować użytkownika, w jaki sposób może on uzyskać dostęp do tych danych.

(21) Produkty mogą być zaprojektowane tak, aby niektóre dane były bezpośrednio dostępne w pamięci urządzenia lub na zdalnym serwerze, do którego dane są przekazywane. Dostęp do pamięci urządzenia można zapewnić za pomocą sieci kablowych lub bezprzewodowych sieci lokalnych podłączonych do publicznie dostępnych usług łączności elektronicznej lub sieci mobilnej. Serwerem może być własny lokalny serwer producenta lub serwer osoby trzeciej lub dostawcy usług w chmurze pełniącego rolę posiadacza danych. Produkty mogą być zaprojektowane w sposób umożliwiający użytkownikowi lub osobie trzeciej przetwarzanie danych z użyciem produktu lub jednostki obliczeniowej producenta.

(22) Wirtualni asystenci odgrywają coraz większą rolę w ramach cyfryzacji otoczenia konsumentów i służą jako łatwy w użyciu interfejs do odtwarzania treści, pozyskiwania informacji lub uruchamiania fizycznych przedmiotów podłączonych do internetu rzeczy. Wirtualni asystenci mogą pełnić rolę jednego punktu dostępu na przykład w środowisku inteligentnego domu i rejestrować znaczne ilości istotnych danych na temat rodzaju interakcji użytkowników z produktami podłączonymi do

internetu rzeczy, w tym produktami wyprodukowanymi przez inne podmioty, i można nimi zastępować interfejsy zapewniane przez producenta, takie jak ekrany dotykowe lub aplikacje na smartfona. Użytkownik może chcieć udostępnić takie dane zewnętrznemu producentowi i umożliwić zastosowanie nowatorskich usług inteligentnego domu. Tacy wirtualni asystenci powinni być objęci prawem dostępu do danych przewidzianym w niniejszym rozporządzeniu również w zakresie danych rejestrowanych przed aktywacją wirtualnego asystenta za pomocą słowa-klucza oraz danych generowanych w trakcie interakcji użytkownika z produktem za pomocą wirtualnego asystenta zapewnionego przez podmiot niebędący producentem danego produktu. Zakres stosowania niniejszego rozporządzenia obejmuje jednak wyłącznie dane wynikające z interakcji między użytkownikiem a produktem za pośrednictwem wirtualnego asystenta. Przedmiotem niniejszego rozporządzenia nie są dane wytworzone przez wirtualnego asystenta niezwiązane z korzystaniem z danego produktu.

(23) Przed zawarciem umowy dotyczącej zakupu, najmu lub leasingu produktu lub świadczenia powiązanej usługi użytkownik musi otrzymać wyraźne i wystarczające informacje wskazujące, w jaki sposób można uzyskać dostęp do generowanych danych. W ramach tego obowiązku zapewnia się przejrzystość w odniesieniu do generowanych danych oraz ułatwia się dostęp dla użytkownika. Ten obowiązek udzielenia informacji nie ma wpływu na obowiązek udzielania informacji osobie, której dane dotyczą, przez administratora danych na podstawie art. 12, 13 i 14 rozporządzenia (UE) 2016/679.

(24) Zgodnie z przepisami niniejszego rozporządzenia posiadacze danych są w określonych okolicznościach zobowiązani do udostępnienia danych. W odniesieniu do przetwarzanych danych osobowych posiadacz danych powinien być administratorem danych na mocy rozporządzenia (UE) 2016/679. Jeżeli użytkownicy są osobami, których dane dotyczą, posiadacze danych powinni być zobowiązani do zapewnienia im dostępu do ich danych oraz udostępnienia tych danych osobom trzecim wskazanym przez użytkownika zgodnie z niniejszym rozporządzeniem. Niniejsze rozporządzenie nie stanowi jednak podstawy prawnej w myśl rozporządzenia (UE) 2016/679 dla zapewniania dostępu do danych osobowych lub ich udostępniania osobie trzeciej przez posiadacza danych na wniosek użytkownika, który nie jest osobą, której dane dotyczą, a ponadto niniejszego rozporządzenia nie należy rozumieć jako nadającego posiadaczowi danych jakiekolwiek nowe prawo do korzystania z danych generowanych w wyniku korzystania z produktu lub powiązanej usługi. Dotyczy to w szczególności sytuacji, w których posiadaczem danych jest producent. W tym przypadku producent powinien wykorzystywać dane nieosobowe na podstawie ustaleń umownych między producentem a użytkownikiem. Umowa ta może stanowić element umowy sprzedaży, najmu lub leasingu zawartej w odniesieniu do danego produktu. Każde zawarte w umowie postanowienie stanowiące, że posiadacz danych może wykorzystywać dane generowane przez użytkownika produktu lub powiązanej usługi, powinno być jasne dla użytkownika, w tym należy jasno określić, w jakim celu posiadacz danych zamierza wykorzystywać dane. Niniejsze rozporządzenie nie powinno uniemożliwiać formułowania warunków umownych skutkujących wykluczeniem lub ograniczeniem wykorzystywania danych lub niektórych ich kategorii przez posiadacza danych. Niniejsze rozporządzenie nie powinno również uniemożliwiać przyjmowania sektorowych wymogów regulacyjnych w prawie Unii lub w przepisach krajowych zgodnych z prawem Unii, które to wymogi spowodowałyby wykluczenie lub ograniczenie korzystania z określonych tego typu

danych przez posiadacza danych w przypadkach uzasadnionych wyraźnie zdefiniowanymi względami porządku publicznego.

(25) W sektorach charakteryzujących się koncentracją małej liczby producentów zaopatrujących użytkowników końcowych użytkownicy mają ograniczone możliwości wymiany danych z tymi producentami. W takich okolicznościach ustalenia umowne mogą nie wystarczyć do osiągnięcia celu, jakim jest wzmocnienie pozycji użytkowników. Dane zwykle pozostają pod kontrolą producentów, przez co użytkownikom trudno jest korzystać z wartości danych generowanych przez sprzęt, który nabyli lub wzięli w leasing. W rezultacie innowacyjne mniejsze przedsiębiorstwa mają ograniczoną możliwość oferowania rozwiązań opartych na danych w sposób konkurencyjny oraz ograniczona jest możliwość rozwoju zróżnicowanej gospodarki opartej o dane w Europie. W niniejszym rozporządzeniu należy zatem rozwijać ostatnie dokonania w konkretnych sektorach, takie jak kodeks postępowania w zakresie udostępniania danych dotyczących rolnictwa na podstawie umownej. Można wprowadzić przepisy sektorowe służące zaspokojeniu potrzeb sektorowych i osiągnięciu celów sektorowych. Ponadto posiadacz danych nie powinien wykorzystywać żadnych danych generowanych w wyniku używania produktu lub powiązanej usługi do pozyskania informacji na temat sytuacji ekonomicznej użytkownika, jego aktywów lub metod produkcji, ani też nie powinien wykorzystywać takich danych w żaden inny sposób, który mógłby osłabić pozycję handlową użytkownika na rynkach, na których prowadzi swoją działalność. Dotyczy to na przykład wykorzystania ze szkodą dla użytkownika wiedzy na temat ogólnych wyników osiąganych w ramach danej działalności gospodarczej lub przez gospodarstwo rolne w prowadzonych z użytkownikiem negocjacjach umownych dotyczących potencjalnego nabycia produktów lub produktów rolniczych użytkownika, lub też na przykład wprowadzania takich informacji do większych baz danych dotyczących określonych rynków w ramach danych zagregowanych (np. baz danych dotyczących wydajności plonów w nadchodzącej porze zbiorów), gdyż takie wykorzystanie danych mogłoby pośrednio negatywnie wpłynąć na użytkownika. Użytkownik powinien otrzymać konieczny interfejs techniczny do zarządzania zgodami, przy czym najlepiej, aby taki interfejs zawierał możliwości udzielenia jednorazowej zgody (np. „Zezwól tylko raz” lub „Zezwól, jeżeli aplikacja lub usługa jest używana”) oraz możliwość cofnięcia zgody.

(26) W umowach między posiadaczem danych a konsumentem będącym użytkownikiem danego produktu lub powiązanej usługi, które generują dane, warunki takiej umowy są objęte zakresem stosowania dyrektywy 93/13/EWG, co ma zapewnić, aby konsument nie podlegał nieuczciwym postanowieniom umownym. W niniejszym rozporządzeniu określono, że nieuczciwe postanowienia umowne nałożone jednostronnie na mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo, zdefiniowane w art. 2 załącznika do zalecenia 2003/361/WE[63], nie powinny być wiążące dla takiego przedsiębiorstwa.

(27) Posiadacz danych może wymagać odpowiedniej identyfikacji użytkownika potrzebnej do zweryfikowania, czy użytkownik jest uprawniony do uzyskania dostępu do danych. W przypadku danych osobowych przetwarzanych przez podmiot przetwarzający dane w imieniu administratora danych posiadacz danych powinien zapewnić, aby podmiot przetwarzający dane otrzymał i przetworzył wniosek o uzyskanie dostępu.

[63] Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

(28) Użytkownik powinien móc korzystać z danych w każdym zgodnym z prawem celu. Obejmuje to przekazanie danych, które użytkownik otrzymał w ramach wykonania prawa przysługującego na mocy niniejszego rozporządzenia, osobie trzeciej oferującej usługę na rynkach niższego szczebla, która może stanowić usługę konkurencyjną względem usługi świadczonej przez posiadacza danych, lub też obejmuje to zlecenie takiego przekazania danych posiadaczowi danych. Posiadacz danych powinien zapewnić, aby dane udostępniane osobie trzeciej były tak samo dokładne, kompletne, wiarygodne i aktualne jak dane generowane w wyniku używania danego produktu lub powiązanej usługi, do których to danych sam posiadacz danych może uzyskać dostęp lub jest uprawniony do uzyskania dostępu. W ramach przetwarzania danych należy przestrzegać wszelkich tajemnic przedsiębiorstwa lub praw własności intelektualnej. Należy zachować zachęty do inwestowania w produkty posiadające funkcje oparte na wykorzystaniu danych pochodzących z czujników, w które wyposażony jest dany produkt. Należy zatem rozumieć, że celem niniejszego rozporządzenia jest propagowanie rozwoju nowych, innowacyjnych produktów lub powiązanych usług, sprzyjanie innowacjom na rynkach niższego szczebla, ale również pobudzenie rozwoju zupełnie nowych usług z wykorzystaniem danych, w tym na podstawie danych generowanych przez różne produkty lub powiązane usługi. Jednocześnie celem jest uniknięcie osłabienia zachęt do inwestowania w rodzaje produktów stanowiących źródło danych, przy czym takie zachęty może na przykład osłabiać wykorzystanie danych do opracowania konkurencyjnego produktu.

(29) Osobą trzecią, której dane są udostępniane, może być przedsiębiorstwo, organizacja badawcza lub organizacja niekomercyjna. 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 żadnych danych generowanych w wyniku używania produktu lub powiązanej usługi do pozyskania informacji na temat sytuacji ekonomicznej takiej osoby trzeciej, jej aktywów lub metod produkcji, ani też nie powinien wykorzystywać takich danych w żaden inny sposób, który mógłby osłabić pozycję handlową takiej osoby trzeciej na rynkach, na których prowadzi ona swoją działalność.

(30) W wyniku korzystania z danego produktu lub powiązanej usługi – zwłaszcza gdy użytkownikiem jest osoba fizyczna – mogą być generowane dane odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą). Przetwarzanie takich danych podlega zasadom określonym w rozporządzeniu (UE) 2016/679, w tym w przypadku gdy w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane[64]. 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 prawo na mocy rozporządzenia (UE) 2016/679 do uzyskania dostępu do dotyczących go danych osobowych, a niniejsze rozporządzenie nie ma wpływu na takie prawo. Zgodnie z niniejszym rozporządzeniem użytkownik będący osobą fizyczną ma również prawo dostępu do wszystkich, osobowych i nieosobowych, danych generowanych przez produkt. Jeżeli użytkownikiem nie jest osoba, której dane dotyczą, tylko przedsiębiorstwo, w tym osoba fizyczna prowadząca jednoosobową działalność gospodarczą, oraz wyłączając przypadki wspólnego użytkowania produktu przez członków gospodarstwa domowego, użytkownik będzie administratorem danych

64 Dz.U. L 303 z 28.11.2018, s. 59.

w rozumieniu rozporządzenia (UE) 2016/679. W związku z powyższym taki użytkownik jako administrator danych zamierzający zażądać udostępnienia danych osobowych generowanych w wyniku korzystania z produktu lub powiązanej usługi musi mieć podstawą prawną do przetwarzania danych przewidzianą w art. 6 ust. 1 rozporządzenia (UE) 2016/679, taką jak zgoda osoby, której dane dotyczą, lub uzasadniony interes. Taki użytkownik powinien zapewnić, aby osoba, której dane dotyczą, została odpowiednio poinformowana o określonych, wyraźnych i 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 określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z tego rozporządzenia. Uznaje się, że po udostępnieniu danych taki użytkownik może z kolei stać się posiadaczem danych, jeżeli spełnia kryteria określone w niniejszym rozporządzeniu, i tym samym będzie podlegać obowiązkom w zakresie udostępniania danych określonym w niniejszym rozporządzeniu.

(31) Dane generowane w wyniku użytkowania produktu lub powiązanej usługi należy udostępniać osobie trzeciej wyłącznie na wniosek użytkownika. W niniejszym rozporządzeniu odpowiednio uzupełnia się prawo przewidziane w art. 20 rozporządzenia (UE) 2016/679. W artykule tym przewidziano, że osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu administratorowi, jeżeli dane te są przetwarzane 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). Osoba, której dane dotyczą, ma również prawo do spowodowania, by dane osobowe zostały przekazane przez jednego administratora bezpośrednio innemu administratorowi, ale wyłącznie wówczas, gdy jest to technicznie możliwe. W art. 20 wskazano, że dotyczy on danych przekazywanych przez osobę, której dane dotyczą, ale nie określono, czy wymaga to aktywnego zachowania ze strony osoby, której dane dotyczą, ani też czy ma on zastosowanie również w sytuacjach, w których dany produkt lub powiązana usługa z założenia w bierny sposób rejestruje zachowanie osoby, której dane dotyczą, lub inne informacje związane z osobą, której dane dotyczą. W niniejszym rozporządzeniu ustanowiono prawo uzupełniające na różne sposoby prawo do otrzymywania i przenoszenia danych osobowych na podstawie art. 20 rozporządzenia (UE) 2016/679. W niniejszym rozporządzeniu użytkownikom przyznaje się prawo dostępu do wszelkich danych generowanych w wyniku korzystania z produktu lub powiązanej usługi oraz udostępniania takich danych osobie trzeciej, niezależnie od charakteru danych osobowych, podziału na czynnie przekazywane dane i dane rejestrowane w sposób bierny oraz niezależnie od podstawy prawnej przetwarzania. W przeciwieństwie do obowiązków technicznych przewidzianych w art. 20 rozporządzenia (UE) 2016/679 w niniejszym rozporządzeniu przewiduje się i zapewnia techniczną możliwość zapewnienia dostępu osobom trzecim do wszystkich rodzajów danych objętych zakresem stosowania niniejszego rozporządzenia, niezależnie od tego, czy chodzi o dane osobowe czy dane nieosobowe. Zgodnie z niniejszym rozporządzeniem posiadacz danych może ponadto określić odpowiednie wynagrodzenie uiszczane przez osoby trzecie, ale nie przez użytkownika, z tytułu wszelkich kosztów poniesionych w związku z udzieleniem bezpośredniego dostępu do danych generowanych przez produkt użytkownika. Brak porozumienia między posiadaczem danych i osobą trzecią co do warunków udzielenia takiego bezpośredniego dostępu w żaden sposób nie może

uniemożliwić osobie, której dane dotyczą, wykonania praw przewidzianych w rozporządzeniu (UE) 2016/679, w tym prawa do przenoszenia danych, poprzez skorzystanie ze środków ochrony prawnej zgodnie z tym rozporządzeniem. W tym kontekście uznaje się, że zgodnie z rozporządzeniem (UE) 2016/679 na podstawie ustaleń umownych posiadacz danych lub osoba trzecia nie mogą przetwarzać szczególnych kategorii danych osobowych.

(32) 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 wyraźnie zażądanej przez użytkownika lub abonenta (lub jedynie w celu wykonania transmisji komunikatu). W ramach dyrektywy 2002/58/WE („dyrektywa o e-prywatności") (i proponowanego rozporządzenia o e-prywatności) chroni się integralność końcowego urządzenia użytkownika, jeżeli chodzi o wykorzystanie możliwości przetwarzania i przechowywania oraz gromadzenia informacji. Urządzenie podłączone do internetu rzeczy uznaje się za urządzenie końcowe, jeżeli jest bezpośrednio lub pośrednio podłączone do publicznej sieci łączności.

(33) Aby uniknąć wykorzystywania użytkowników, osoby trzecie, którym dane udostępniono na wniosek użytkownika, powinny przetwarzać dane wyłącznie do celów uzgodnionych z użytkownikiem i udostępniać te dane innej osobie trzeciej wyłącznie wówczas, gdy jest to niezbędne do świadczenia usługi zażądanej przez użytkownika.

(34) Zgodnie z zasadą minimalizacji danych osoba trzecia powinna jedynie uzyskać dostęp do informacji dodatkowych, które są niezbędne do świadczenia usługi zażądanej przez użytkownika. Po uzyskaniu dostępu do danych osoba trzecia powinna przetwarzać otrzymane dane wyłącznie do celów uzgodnionych z użytkownikiem bez ingerencji ze strony posiadacza danych. Odmówienie udzielenia 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 przez użytkownika na taki dostęp. Osoba trzecia nie może w żaden sposób zmuszać ani oszukiwać użytkownika ani też nim manipulować poprzez podważenie lub ograniczenie autonomii, zdolności decyzyjnej lub wyborów użytkownika, w tym za pomocą cyfrowego interfejsu z użytkownikiem. W tym kontekście osoby trzecie nie powinny stosować tak zwanych zwodniczych interfejsów w ramach projektowania swoich cyfrowych interfejsów. Zwodnicze interfejsy to techniki projektowania służące do wymuszania na konsumentach podejmowania decyzji, które mają dla nich negatywne skutki, lub oszukiwania konsumentów w celu skłonienia ich do podejmowania takich decyzji. Te techniki manipulacji mogą być wykorzystywane do skłonienia użytkowników, w szczególności konsumentów podatnych na zagrożenia, do niechcianych zachowań lub nakłaniania ich do podejmowania decyzji dotyczących transakcji ujawniania danych lub też do nieobiektywnego wpływania na decyzje użytkowników usługi w sposób podważający lub ograniczający ich autonomię, zdolność decyzyjną i wybór. Powszechne i uzasadnione praktyki handlowe zgodne z prawem Unii jako takie nie powinny być uznawane za zwodnicze interfejsy. Osoby trzecie powinny wywiązywać się ze swoich obowiązków określonych w stosownych przepisach prawa Unii, w szczególności powinny przestrzegać wymogów określonych w dyrektywie 2005/29/WE, dyrektywie 2011/83/UE, dyrektywie 2000/31/WE i dyrektywie 98/6/WE.

(35) Osoba trzecia nie powinna ponadto wykorzystywać danych do profilowania osób fizycznych, chyba że takie czynności przetwarzania są ściśle niezbędne do świadczenia usługi zażądanej przez użytkownika. Wymóg usunięcia danych, które nie są już wymagane do celu uzgodnionego z użytkownikiem, stanowi uzupełnienie prawa do usunięcia danych przysługującego osobie, której dane dotyczą, na podstawie art. 17 rozporządzenia (UE) 2016/679. Jeżeli osoba trzecia jest dostawcą usługi pośrednictwa w zakresie danych w rozumieniu [aktu w sprawie zarządzania danymi], zastosowanie mają zabezpieczenia przewidziane w tym rozporządzeniu z myślą o osobie, której dane dotyczą. Osoba trzecia może wykorzystywać dane do opracowania nowego i innowacyjnego produktu lub nowej, innowacyjnej powiązanej usługi, ale nie do opracowania produktu konkurencyjnego.

(36) Przedsiębiorstwom typu start-up, małym i średnim przedsiębiorstwom i 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 zakres odpowiednich obowiązków był jak najbardziej proporcjonalny w celu uniknięcia nadmiernego rozszerzenia zakresu stosowania rozporządzenia. Jednocześnie pojawiła się mała liczba bardzo dużych przedsiębiorstw posiadających znaczną siłę gospodarczą w gospodarce cyfrowej w wyniku koncentracji i agregacji wielkich ilości danych oraz dzięki technicznej infrastrukturze pozwalającej na monetyzację danych. Są to między innymi przedsiębiorstwa zapewniające 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 w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych)] ma na celu skorygowanie tych braków i zakłóceń równowagi poprzez umożliwienie Komisji wyznaczenia dostawcy jako strażnika dostępu, a określono w nim szereg obowiązków takich wyznaczonych strażników dostępu, w tym zakaz łączenia niektórych danych bez uzyskania zgody, oraz obowiązek zapewnienia efektywnego wykonania prawa do przenoszenia danych na podstawie art. 20 rozporządzenia (UE) 2016/679. Zgodnie z [rozporządzeniem w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych)] i mając na uwadze wyjątkową zdolność tych przedsiębiorstw do pozyskiwania danych, uwzględnienie takich przedsiębiorstw pełniących rolę strażników dostępu wśród beneficjentów prawa dostępu do danych nie byłoby konieczne do osiągnięcia celu niniejszego rozporządzenia i tym samym byłoby nieproporcjonalne względem posiadaczy danych, na których nałożono takie obowiązki. Oznacza to, że przedsiębiorstwo świadczące podstawowe usługi platformowe, które zostało wyznaczone jako strażnik dostępu, nie może żądać ani uzyskać dostępu do danych użytkownika generowanych w wyniku korzystania z produktu, powiązanej usługi lub wirtualnego asystenta na podstawie przepisów rozdziału II niniejszego rozporządzenia. Przez przedsiębiorstwo świadczące podstawowe usługi platformowe, które zostało wyznaczone jako strażnik dostępu na podstawie aktu o rynkach cyfrowych, rozumie się wszystkie podmioty prawne należące do grupy przedsiębiorstw, w której jeden podmiot prawny świadczy podstawową usługę platformową. Ponadto osoby trzecie, którym dane są udostępniane na wniosek użytkownika, nie mogą udostępniać tych danych wyznaczonemu 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 wyznaczonego

strażnika dostępu. Takie wykluczenie strażników dostępu z zakresu stosowania prawa dostępu na mocy niniejszego rozporządzenia nie oznacza, że przedsiębiorstwa te nie mogą pozyskiwać danych na inne zgodne z prawem sposoby.

(37) Biorąc pod uwagę obecny stan rozwoju technologii, nakładanie dalszych obowiązków w zakresie projektowania produktów wytworzonych lub zaprojektowanych przez mikroprzedsiębiorstwa i małe przedsiębiorstwa oraz powiązanych usług świadczonych przez takie przedsiębiorstwa wiąże się z nadmiernym obciążeniem. Nie dotyczy to jednak sytuacji, w której wyprodukowanie lub zaprojektowanie danego produktu zostaje zlecone mikroprzedsiębiorstwu lub małemu przedsiębiorstwu w ramach podwykonawstwa. W takich sytuacjach przedsiębiorstwo, które zleciło podwykonawstwo mikroprzedsiębiorstwu lub małemu przedsiębiorstwu, jest w stanie zapewnić podwykonawcy odpowiednie wynagrodzenie. Mikroprzedsiębiorstwo lub małe przedsiębiorstwo może jednak podlegać wymogom określonym w niniejszym rozporządzeniu jako posiadacz danych, jeżeli nie jest producentem danego produktu ani dostawcą powiązanych usług.

(38) Niniejsze rozporządzenie zawiera ogólne zasady dotyczące dostępu stosowane zawsze, gdy posiadacz danych jest zobowiązany z mocy prawa do udostępnienia danych odbiorcy danych. Takiego dostępu należy udzielać na sprawiedliwych, uzasadnionych, niedyskryminacyjnych i przejrzystych warunkach, aby zapewnić spójność praktyk w zakresie udostępniania danych na rynku wewnętrznym, w tym między sektorami, oraz aby zachęcać do stosowania uczciwych praktyk w zakresie udostępniania danych i promować takie praktyki nawet w obszarach, w których nie przewidziano takiego prawa do uzyskania dostępu do danych. Te ogólne zasady dotyczące dostępu nie mają zastosowania do obowiązków w zakresie udostępniania danych na podstawie rozporządzenia (UE) 2016/679. Zasady te nie mają wpływu na dobrowolne udostępnianie danych.

(39) Na podstawie zasady swobody zawierania umów strony powinny móc swobodnie negocjować szczegółowe warunki udostępniania danych zawarte w ich umowach, w ramach ogólnych zasad dostępu w zakresie udostępniania danych.

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

(41) Ze względu na brak informacji na temat warunków poszczególnych umów odbiorcom danych trudno jest ocenić, czy warunki udostępniania danych są niedyskryminacyjne, i celem zrekompensowania im braku tych informacji ciężar udowodnienia, że postanowienia umowne są niedyskryminacyjne, powinien spoczywać na posiadaczu danych. Nie uznaje się, że stosowanie przez posiadacza danych różnych postanowień umownych dotyczących udostępniania danych lub różnego wynagrodzenia stanowi niezgodną z prawem dyskryminację, jeżeli różnice te są uzasadnione obiektywnymi względami. Obowiązki te nie naruszają przepisów rozporządzenia (UE) 2016/679.

(42) Aby zachęcać do dalszych inwestycji w generowanie cennych danych, w tym inwestycji w stosowne narzędzia techniczne, w niniejszym rozporządzeniu określono zasadę, zgodnie z którą posiadacz danych może zażądać odpowiedniego wynagrodzenia, gdy jest zobowiązany na mocy prawa do udostępnienia danych odbiorcy danych. Przepisów tych nie należy rozumieć jako przepisów określających zapłatę za same dane, ale raczej – w przypadku mikroprzedsiębiorstw, małych lub

średnich przedsiębiorstw – zapłatę za poniesione koszty i wymagane inwestycje związane z udostępnieniem danych.

(43) W uzasadnionych przypadkach, w tym w związku z koniecznością zabezpieczenia udziału konsumentów i konkurencyjności lub promowania innowacyjności na niektórych rynkach, w prawie Unii lub przepisach krajowych wykonujących prawo Unii można przewidzieć uregulowane wynagrodzenie za udostępnianie określonego rodzaju danych.

(44) Na potrzeby ochrony mikroprzedsiębiorstw i małych lub średnich przedsiębiorstw przed nadmiernymi obciążeniami ekonomicznymi, przez które przedsiębiorstwom tym z handlowego punktu widzenia byłoby zbyt trudno rozwijać i realizować innowacyjne modele biznesowe, wypłacane przez nie wynagrodzenie za udostępnienie danych nie powinno przekraczać bezpośredniego kosztu udostępnienia danych i musi być niedyskryminacyjne.

(45) Koszty bezpośrednie związane z udostępnianiem danych to koszty, które trzeba ponieść w związku ze zwielokrotnieniem danych, rozpowszechnianiem danych za pośrednictwem środków elektronicznych i przechowywaniem danych, ale nie z gromadzeniem lub tworzeniem danych. Koszty bezpośrednie związane z udostępnianiem danych powinny ograniczać się do części kosztów, która wiąże się z danym pojedynczym wnioskiem, mając na uwadze, że niezbędne interfejsy techniczne lub powiązane oprogramowanie i łączność posiadacz danych będzie musiał zapewnić na stałe. Koszty związane z regularnym lub powtarzającym się udostępnianiem danych w ramach stosunków biznesowych można ograniczyć poprzez dokonywanie długoterminowych ustaleń między posiadaczami danych i odbiorcami danych, na przykład poprzez przyjęcie modelu abonenckiego.

(46) Nie ma potrzeby interwencji w przypadku udostępniania danych 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 każde rozsądne wynagrodzenie, biorąc pod uwagę takie czynniki jak ilość, format, charakter danych lub ich podaż i popyt na nie, a także koszty zgromadzenia danych i ich udostępnienia odbiorcy danych.

(47) Przejrzystość stanowi ważną zasadę potrzebną do zapewnienia, aby wynagrodzenie żądane przez posiadacza danych było rozsądne lub – jeżeli odbiorcą danych jest mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo – aby kwota wynagrodzenia nie przekraczała kosztów bezpośrednio związanych z udostępnieniem danych odbiorcy danych w związku z danym konkretnym wnioskiem. Aby odbiorca danych był w stanie ocenić i zweryfikować, czy wynagrodzenie jest zgodne z wymogami określonymi w niniejszym rozporządzeniu, posiadacz danych powinien udzielić odbiorcy danych informacji na tyle szczegółowych, aby można było obliczyć wynagrodzenie.

(48) 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 zaufania do udostępniania danych. Jeżeli strony nie są w stanie uzgodnić sprawiedliwych, rozsądnych i niedyskryminujących warunków udostępniania danych, organy rozstrzygania sporów powinny zaoferować stronom proste, szybkie i tanie rozwiązanie.

(49) Aby uniknąć sytuacji, w której ten sam spór zostaje skierowany do rozpatrzenia przez co najmniej dwa organy rozstrzygania sporów, zwłaszcza w sytuacji transgranicznej, organ rozstrzygania sporów powinien mieć możliwość odrzucenia wniosku o rozstrzygnięcie sporu, który został już wniesiony do innego organu rozstrzygania sporów bądź do sądu lub trybunału państwa członkowskiego.

(50) Stronom postępowania w sprawie rozstrzygnięcia sporu nie można uniemożliwiać wykonania przysługującego im podstawowego prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu. Dlatego też decyzja o przekazaniu sporu do rozpatrzenia przez organ rozstrzygający spory nie powinna skutkować utratą przez takie strony prawa do wniesienia sprawy do sądu lub trybunału państwa członkowskiego.

(51) Jeżeli jedna ze stron ma silniejszą pozycję negocjacyjną, istnieje ryzyko, że strona ta wykorzysta swoją pozycję ze szkodą dla drugiej umawiającej się strony w ramach negocjacji dostępu do danych oraz sprawi, że dostęp do danych będzie komercyjnie mniej opłacalny, a czasem nawet ekonomicznie niemożliwy. Taki brak równowagi kontraktowej jest szczególnie szkodliwy dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw nieposiadających istotnej zdolności do negocjowania warunków dostępu do danych, które to przedsiębiorstwa ze względu na brak innego 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 korzystanie z nich lub odpowiedzialność i środki ochrony prawnej w zakresie naruszenia lub wygaśnięcia obowiązków dotyczących danych nie powinny być wiążące dla mikroprzedsiębiorstw i małych lub średnich przedsiębiorstw, jeżeli takie postanowienia jednostronnie nałożono na te przedsiębiorstwa.

(52) W przepisach dotyczących postanowień umownych należy uwzględnić zasadę swobody zawierania umów będącą podstawową ideą, jeżeli chodzi o stosunki między przedsiębiorstwami. Dlatego też analizie nieuczciwego charakteru nie powinny podlegać wszystkie postanowienia umowne, a jedynie te, które zostały jednostronnie nałożone na mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa. Dotyczy to stosowania zasady „przyjmij albo zrezygnuj” – w takiej sytuacji mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo nie jest w stanie wywrzeć wpływu na treść postanowienia umownego zaproponowanego przez drugą stronę pomimo prób negocjacji treści takiego postanowienia. Za postanowienie umowne nałożone jednostronnie nie należy uznać postanowienia umownego, które zostało zwyczajnie przedstawione przez jedną stronę i zaakceptowane przez mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo ani też postanowienia wynegocjowanego i następnie uzgodnionego na zasadzie zmiany między umawiającymi się stronami.

(53) 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 korzystania z nich, a także odpowiedzialności lub środków ochrony prawnej w zakresie naruszenia i wygaśnięcia obowiązków dotyczących danych. Analiza nieuczciwego charakteru określona w niniejszym rozporządzeniu nie powinna mieć zastosowania do innych części tej samej umowy, niezwiązanych z udostępnianiem danych.

(54) Kryteria służące do identyfikacji nieuczciwych postanowień umownych należy stosować wyłącznie wobec nieproporcjonalnych postanowień umownych,

w przypadku których dochodzi 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 przedsiębiorstwami, zwyczajnie odzwierciedla zasadę swobody zawierania umów i nadal powinna obowiązywać.

(55) Jeżeli dane postanowienie umowne nie widnieje w wykazie postanowień, które zawsze uznaje się za nieuczciwe albo w odniesieniu do których przyjmuje się domniemanie ich nieuczciwości, zastosowanie ma ogólny przepis dotyczący nieuczciwego charakteru. W tym względzie postanowienia wymienione jako nieuczciwe postanowienia umowne powinny służyć jako kryteria interpretacji ogólnego przepisu dotyczącego nieuczciwego charakteru. Ponadto modelowe postanowienia umowne w umowach dotyczących udostępniania danych między przedsiębiorstwami opracowane i rekomendowane przez Komisję mogą ułatwić stronom będącym podmiotami komercyjnymi negocjowanie umów.

(56) W sytuacji wystąpienia wyjątkowej potrzeby może być konieczne wykorzystanie danych posiadanych przez przedsiębiorstwo przez organy sektora publicznego lub instytucje, agencje lub organy Unii w celu podjęcia działania w związku z niebezpieczeństwem publicznym lub w innych wyjątkowych przypadkach. Organizacje prowadzące badania naukowe i organizacje finansujące badania naukowe także mogą być organami sektora publicznego lub podmiotami prawa publicznego. Aby zmniejszyć obciążenie przedsiębiorstw, należy zwolnić mikroprzedsiębiorstwa i małe przedsiębiorstwa z obowiązku przekazywania danych organom sektora publicznego oraz instytucjom, agencjom lub organom Unii w sytuacjach wystąpienia wyjątkowej potrzeby.

(57) W przypadkach wystąpienia niebezpieczeństwa publicznego – takiego jak stan zagrożenia zdrowia publicznego, sytuacje wyjątkowe związane z degradacją środowiska i poważne klęski żywiołowe, w tym sytuacje pogarszane przez skutki zmiany klimatu, a także poważne katastrofy spowodowane przez człowieka, takie jak poważne cyberincydenty – interes publiczny wynikający z użycia danych będzie nadrzędny względem interesów posiadacza danych związanych ze swobodnym dysponowaniem danymi, które posiada. W takim przypadku posiadacze danych powinni być zobowiązani do udostępnienia danych organom sektora publicznego lub instytucjom, agencjom lub organom Unii na ich wniosek. Występowanie niebezpieczeństwa publicznego ustala się na podstawie odpowiednich procedur stosowanych w państwach członkowskich lub przez odpowiednie organizacje międzynarodowe.

(58) Wyjątkowa potrzeba może wystąpić również w sytuacji, w której organ sektora publicznego może wykazać, że dane są niezbędne do zapobieżenia niebezpieczeństwu publicznemu albo do wsparcia przywrócenia stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego, w okolicznościach wystarczająco zbliżonych do danego rodzaju niebezpieczeństwa publicznego. Jeżeli wyjątkowa potrzeba nie jest uzasadniona koniecznością podjęcia działań w reakcji na niebezpieczeństwo publiczne, działań służących zapobieżeniu niebezpieczeństwu publicznemu lub działań wspierających przywracanie stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego, organ sektora publicznego lub instytucja, agencja lub organ Unii powinny wykazać, że w przypadku braku terminowego udostępnienia żądanych danych lub ich wykorzystania dana jednostka nie będzie mogła skutecznie zrealizować konkretnego zadania leżącego w interesie publicznym i wyraźnie wskazanego w prawie. Taka wyjątkowa potrzeba może pojawić się również w innych

sytuacjach, na przykład w związku z terminowym zestawieniem danych w ramach statystyki publicznej, gdy dane nie są dostępne w inny sposób lub gdy będzie to oznaczało znaczne ograniczenie obciążenia nakładanego na respondentów. Jeżeli nie zachodzi konieczność podjęcia działań w reakcji na niebezpieczeństwo publiczne, działań służących zapobieżeniu niebezpieczeństwu publicznemu lub działań wspierających przywracanie stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego, organ sektora publicznego lub instytucja, agencja lub organ Unii będą musiały jednocześnie wykazać, że nie istnieje żaden alternatywny sposób pozyskania żądanych danych oraz że danych tych nie można pozyskać w odpowiednim czasie poprzez określenie niezbędnych obowiązków dotyczących przekazywania danych w drodze nowych przepisów.

(59) Niniejsze rozporządzenie nie powinno dotyczyć, ani wykluczać, dobrowolnych ustaleń dotyczących wymiany danych między podmiotami prywatnymi i publicznymi. Niniejsze rozporządzenie nie powinno mieć wpływu na obowiązki dotyczące przekazywania danych przez posiadaczy danych w sytuacjach, w których nie zachodzi wyjątkowa potrzeba, w szczególności gdy zakres danych i posiadaczy danych jest znany, a dane można wykorzystywać regularnie, tak jak ma to miejsce w przypadku obowiązków sprawozdawczych i obowiązków związanych z rynkiem wewnętrznym. Niniejsze rozporządzenie nie powinno mieć również wpływu na wymogi dotyczące dostępu do danych w celu weryfikacji przestrzegania mających zastosowanie przepisów, w tym w przypadkach, w których organy sektora publicznego zlecają przeprowadzenie weryfikacji zgodności jednostkom niebędącym organami sektora publicznego.

(60) 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 gromadzenia danych do celów celnych bądź podatkowych organy sektora publicznego i instytucje, agencje i organy Unii powinny korzystać z uprawnień nadanych im w przepisach sektorowych. Niniejsze rozporządzenie nie ma zatem wpływu na instrumenty służące do udostępniania danych, uzyskiwania do nich dostępu i ich wykorzystania w tych obszarach.

(61) Na szczeblu UE muszą funkcjonować proporcjonalne, ograniczone i przewidywalne ramy udostępniania danych przez posiadaczy danych, w przypadkach występowania wyjątkowej potrzeby, organom sektora publicznego i instytucjom, agencjom lub organom Unii w celu zapewnienia pewności prawa i ograniczenia do minimum obciążeń administracyjnych nakładanych na przedsiębiorstwa. W tym celu wnioski o udostępnienie danych przedstawiane posiadaczom danych przez organy sektora publicznego i przez instytucje, agencje i organy Unii powinny być przejrzyste i proporcjonalne pod względem zakresu treści i poziomu szczegółowości. Należy wyraźnie i konkretnie wskazać cel wniosku i planowane wykorzystanie żądanych danych, a jednocześnie należy zapewnić odpowiednią elastyczność tak, aby podmiot przedstawiający wniosek mógł realizować swoje zadania leżące w interesie publicznym. We wniosku należy również wziąć pod uwagę uzasadnione interesy przedsiębiorstw będących adresatami tego wniosku. Należy ograniczyć do minimum obciążenie nakładane na posiadaczy danych poprzez zobowiązanie podmiotów występujących z wnioskiem do przestrzegania zasady jednorazowości, zgodnie z którą o przekazanie tych samych danych może wystąpić tylko jednokrotnie nie więcej niż jeden organ sektora publicznego, jedna instytucja lub agencja Unii lub jeden organ Unii, jeżeli dane te są niezbędne do podjęcia działania w związku

z niebezpieczeństwem publicznym. Celem zapewnienia przejrzystości wnioski o udostępnienie danych przedstawione przez organy sektora publicznego lub przez instytucje, agencje lub organy Unii powinny zostać bez zbędnej zwłoki podane do wiadomości publicznej przez podmiot wnioskujący o udostępnienie danych oraz należy zapewnić, aby wszystkie wnioski uzasadnione występowaniem niebezpieczeństwa publicznego były publicznie udostępniane w internecie.

(62) Celem obowiązku przekazywania danych jest zapewnienie, aby organy sektora publicznego oraz instytucje, agencje lub organy Unii dysponowały niezbędną wiedzą na potrzeby podejmowania działań w reakcji na niebezpieczeństwo publiczne, działań służących zapobieżeniu niebezpieczeństwu publicznemu lub działań służących przywracaniu stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego lub na potrzeby zachowania zdolności do realizacji konkretnego zadania wyraźnie wskazanego w prawie. Wśród danych uzyskanych przez te podmioty mogą znajdować się szczególnie chronione informacje handlowe. Z tego względu dane udostępniane na podstawie niniejszego rozporządzenia nie powinny być objęte zakresem stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024[65] i nie należy uznawać, że są to otwarte dane, które mogą być ponownie wykorzystane przez osoby trzecie. Nie powinno to mieć jednak wpływu na stosowanie dyrektywy (UE) 2019/1024 do ponownego wykorzystania danych statystyki publicznej, przy której tworzeniu wykorzystano dane uzyskane na podstawie niniejszego rozporządzenia, pod warunkiem że ponowne wykorzystanie nie dotyczy danych bazowych. Ponadto nie powinno to mieć wpływu na możliwość udostępniania danych do celów prowadzenia badań lub gromadzenia danych w ramach statystyki publicznej, pod warunkiem że spełnione są warunki określone w niniejszym rozporządzeniu. Organy sektora publicznego powinny również mieć możliwość udostępniania danych uzyskanych na podstawie niniejszego rozporządzenia innym organom sektora publicznego w celu zaspokojenia wyjątkowych potrzeb, w związku z którymi wystosowano wniosek o udostępnienie danych.

(63) Posiadacze danych powinni móc zwrócić się o zmianę wniosku przedstawionego przez organ sektora publicznego lub instytucję, agencję i organ Unii albo o anulowanie takiego wniosku w terminie 5 lub 15 dni roboczych w zależności od charakteru wyjątkowej potrzeby, na którą powołano się we wniosku. W przypadku wniosków składanych w związku z wystąpieniem niebezpieczeństwa publicznego nieudostępnienie danych powinno być uzasadnione w sytuacji, w której można wykazać, że podobny lub identyczny wniosek został już wcześniej złożony w tym samym celu przez inny organ sektora publicznego lub inną instytucję lub agencję Unii lub inny organ Unii. Posiadacz danych, który odrzuca wniosek lub dąży do jego zmiany, powinien przedstawić stosowne uzasadnienie odrzucenia wniosku organowi sektora publicznego lub instytucji, agencji lub organowi Unii wnioskującym o udostępnienie danych. Jeżeli w odniesieniu do żądanych zestawów danych mają zastosowanie prawa *sui generis* do baz danych przewidziane w dyrektywie 96/6/WE Parlamentu Europejskiego i Rady[66], posiadacze danych powinni korzystać z przysługujących im praw w sposób, który nie uniemożliwia organowi sektora

---

65 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).

66 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).

publicznego i instytucjom, agencjom lub organom Unii uzyskania lub udostępnienia danych zgodnie z niniejszym rozporządzeniem.

(64) Jeżeli uwzględnienie danych osobowych w danych udostępnianych organowi sektora publicznego lub instytucji, agencji lub organowi Unii jest ściśle niezbędne, należy przestrzegać mających zastosowanie przepisów dotyczących ochrony danych osobowych, a udostępniając i następnie wykorzystując dane, należy zapewnić zabezpieczenia chroniące prawa i interesy osób fizycznych, których dane te dotyczą. Organ występujący z wnioskiem o udostępnienie danych powinien wykazać, że dane te są ściśle niezbędne, oraz przedstawić konkretne i ograniczone cele przetwarzania. Przed udostępnieniem danych posiadacz danych powinien poczynić racjonalne kroki w celu anonimizacji danych lub – jeżeli anonimizacja danych jest niemożliwa – zastosować środki technologiczne, takie jak pseudonimizacja i agregacja.

(65) Dane udostępniane organom sektora publicznego i instytucjom, agencjom i organom Unii na podstawie występowania wyjątkowej potrzeby należy wykorzystywać wyłącznie w celu wskazanym we wniosku o ich udostępnienie, chyba że posiadacz danych, który udostępnił dane, wyraził wyraźną zgodę na wykorzystanie tych danych do innych celów. Dane należy zniszczyć, gdy tylko przestaną być potrzebne do celu wskazanego we wniosku, chyba że uzgodniono inaczej, a o ich zniszczeniu należy powiadomić posiadacza danych.

(66) Ponownie wykorzystując dane przekazane przez posiadaczy danych, organy sektora publicznego oraz instytucje, agencje lub organy Unii powinny przestrzegać zarówno obowiązujących przepisów, jak i zobowiązań umownych, którym podlega posiadacz danych. Jeżeli ujawnienie tajemnic przedsiębiorstwa posiadacza danych organom sektora publicznego lub instytucjom, agencjom lub organom Unii jest ściśle niezbędne do osiągnięcia celu wskazanego we wniosku o udostępnienie danych, posiadaczowi danych należy zagwarantować zachowanie poufności takich ujawnianych danych.

(67) Jeżeli konieczna jest ochrona istotnego dobra publicznego, jak na przykład w przypadku reagowania na niebezpieczeństwo publiczne, od organu sektora publicznego lub instytucji, agencji lub organu Unii nie należy oczekiwać wypłaty przedsiębiorstwom wynagrodzenia za przekazane dane. Niebezpieczeństwo publiczne należy do rzadkich zdarzeń i nie wszystkie przypadki wystąpienia takiego niebezpieczeństwa wymagają wykorzystania danych będących w posiadaniu przedsiębiorstw. Skorzystanie z przepisów niniejszego rozporządzenia przez organy sektora publicznego lub instytucje, agencje lub organy Unii prawdopodobnie nie będzie zatem miało negatywnego wpływu na działalność gospodarczą prowadzoną przez posiadaczy danych. Ponieważ jednak częściej mogą występować przypadki występowania wyjątkowej potrzeby niezwiązane z koniecznością reagowania na niebezpieczeństwo publiczne – w tym przypadki zapobiegania niebezpieczeństwu publicznemu lub przywracania stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego – w takich przypadkach posiadacze danych powinni być upoważnieni do otrzymania rozsądnego wynagrodzenia, którego kwota nie powinna przekraczać technicznych i organizacyjnych kosztów poniesionych w związku ze spełnieniem wniosku i rozsądnej marży wymaganej w celu udostępnienia danych organowi sektora publicznego lub instytucji, agencji lub organowi Unii. Wynagrodzenia nie należy rozumieć jako płatności za same dane i jako wynagrodzenia obowiązkowego.

(68) Organ sektora publicznego lub instytucja, agencja lub organ Unii może udostępnić dane uzyskane na podstawie wniosku innym podmiotom lub osobom, jeżeli wymaga tego prowadzenie działań naukowych lub analitycznych, których nie jest w stanie

przeprowadzić samodzielnie. Takie dane można również udostępniać w takich samych okolicznościach krajowym urzędom statystycznym i Eurostatowi do celów tworzenia statystyki publicznej. Takie działania naukowe powinny jednak być zgodne z celem wskazanym we wniosku o udostępnienie danych, a posiadacza danych należy powiadomić o dalszym udostępnieniu danych, które przekazał. Osoby fizyczne przeprowadzające badania lub organizacje badawcze, którym dane te mogą być udostępnianie, powinny prowadzić działalność o charakterze niekomercyjnym albo prowadzić działalność w kontekście misji realizacji interesu publicznego uznanej przez państwo. Do celów niniejszego rozporządzenia za organizacje badawcze nie uznaje się organizacji znajdujących się pod decydującym wpływem przedsiębiorstw komercyjnych, które mogą sprawować kontrolę nad daną organizacją ze względu na okoliczności strukturalne, przez co może dochodzić do udzielania preferencyjnego dostępu do wyników badań.

(69) Podstawowym warunkiem stworzenia bardziej konkurencyjnego rynku charakteryzującego się mniejszymi barierami wejścia nowych dostawców usług jest zapewnienie, aby klienci używający usługi przetwarzania danych, w tym usługi w chmurze i usługi przetwarzania brzegowego, mogli przechodzić od jednej do drugiej usługi przetwarzania danych z zachowaniem minimalnego poziomu funkcjonalności danej usługi.

(70) W rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1807 dostawców usług wspiera się w skutecznym opracowywaniu i wdrażaniu samoregulacyjnych kodeksów postępowania obejmujących między innymi najlepsze praktyki w zakresie ułatwiania zmiany dostawcy usług i przenoszenia danych. Mając na uwadze ograniczoną skuteczność samoregulacyjnych ram opracowanych w związku z tym rozporządzeniem oraz ogólną niedostępność otwartych standardów i interfejsów, konieczne jest przyjęcie zestawu minimalnych obowiązków regulacyjnych wobec dostawców usług przetwarzania danych w celu wyeliminowania umownych, ekonomicznych i technicznych barier utrudniających skuteczne przechodzenie od jednych do drugich usług przetwarzania danych.

(71) Usługi przetwarzania danych powinny obejmować usługi, które umożliwiają szeroki dostęp zdalny na żądanie do skalowalnego i elastycznego zbioru rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania. Pojęcie „zasoby obliczeniowe” obejmuje takie zasoby jak sieci, serwery lub inną wirtualną lub fizyczną infrastrukturę, systemy operacyjne, 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 sieciowy magazyn danych, bez żadnej ingerencji człowieka ze strony dostawcy usługi, można określić jako administrowanie na żądanie. Pojęcia „szeroki dostęp zdalny” używa się do opisu sytuacji, gdy 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 usługi przetwarzania danych niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania. Pojęcia „elastyczny zbiór” 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 „wspólne wykorzystywanie” 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 gromadzenia danych, na przykład w podłączonym 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.

(72) Niniejsze rozporządzenie ma ułatwić przechodzenie od jednej do drugiej usługi przetwarzania danych, przy czym takie przejście obejmuje wszystkie warunki i działania niezbędne do rozwiązania przez klienta umowy dotyczącej danej usługi przetwarzania danych, zawarcia co najmniej jednej nowej umowy z innymi dostawcami usług przetwarzania danych, przeniesienia wszystkich posiadanych aktywów cyfrowych, w tym danych, do takich innych dostawców i kontynuacji korzystania z danych usług w nowym środowisku i z zachowaniem równoważności funkcjonalnej. Aktywa cyfrowe oznaczają elementy w formacie cyfrowym, do których użytkowania klient ma prawo, w tym dane, aplikacje, maszyny wirtualne i inne elementy stanowiące wyraz technologii wirtualizacji, takie jak pojemniki. Równoważność funkcjonalna oznacza zachowanie minimalnego poziomu funkcjonalności danej usługi po przejściu na nową usługę i należy uznać, że jej zapewnienie jest technicznie możliwe zawsze, gdy obie usługi przetwarzania danych – usługa pierwotna i docelowa – obejmują (częściowo lub w całości) ten sam rodzaj usługi. Zgodnie z przepisami niniejszego rozporządzenia dotyczącymi przechodzenia na nowe usługi możliwość przenoszenia powinna również dotyczyć metadanych wygenerowanych w wyniku korzystania z usługi przez klienta.

(73) Jeżeli dostawcy usług przetwarzania danych są z kolei klientami korzystającymi z usług przetwarzania danych dostarczanych przez dostawcę zewnętrznego, sami będą korzystać ze skuteczniejszej możliwości zamiany usług, a jednocześnie niezmiennie będą podlegać obowiązkom określonym w niniejszym rozporządzeniu odnoszącym się do ich własnej oferty usług.

(74) Dostawcy usług przetwarzania danych powinni być zobowiązani do zapewnienia wszelkiej pomocy i wszelkiego wsparcia, które są potrzebne do zapewnienia skuteczniejszego procesu zamiany bez konieczności opracowania przez takich dostawców usług przetwarzania danych nowych kategorii usług w ramach infrastruktury informatycznej poszczególnych dostawców usług przetwarzania danych lub w oparciu o taką infrastrukturę w celu zagwarantowania równoważności funkcjonalnej w środowisku innym niż ich własne systemy. Dostawcy usług są jednak zobowiązani do zapewnienia wszelkiej pomocy i wszelkiego wsparcia, które są potrzebne do zapewnienia skuteczniejszego procesu zamiany. 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[67].

(75) Aby ułatwić zamianę usług przetwarzania danych, dostawcy takich usług powinni rozważyć korzystanie z narzędzi wdrażania lub zapewniania przestrzegania przepisów, w szczególności narzędzi publikowanych przez Komisję w postaci zbioru przepisów dotyczących usług w chmurze. W szczególności standardowe klauzule umowne sprzyjają wzrostowi zaufania do usług przetwarzania danych, tworzeniu lepiej wyważonych stosunków między użytkownikami a dostawcami usług oraz poprawie pewności prawa w kwestii warunków mających zastosowanie do przejścia na inne usługi przetwarzania danych. W tym kontekście użytkownicy i dostawcy usług powinni rozważyć zastosowanie standardowych klauzul umownych opracowanych przez odpowiednie organy lub grupy ekspertów ustanowione na mocy prawa Unii.

(76) Otwarte specyfikacje i normy w zakresie interoperacyjności opracowane zgodnie z pkt 3 i 4 załącznika II do rozporządzenia (UE) 1025/2021 w obszarze interoperacyjności i możliwości przenoszenia umożliwiają budowanie sprawnie funkcjonującego środowiska chmury obliczeniowej bazującego na usługach świadczonych przez wielu dostawców, co stanowi kluczowy wymóg dotyczący otwartych innowacji w europejskiej gospodarce opartej o dane. Ponieważ nie wykazano, aby procesy rynkowe mogły skutkować ustanowieniem specyfikacji i norm technicznych umożliwiających zapewnienie skutecznej interoperacyjności usług w chmurze na poziomie PaaS (platforma jako usługa) i SaaS (oprogramowanie jako usługa), 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, zwłaszcza w przypadku rodzajów usług, w odniesieniu do których nie opracowano jeszcze takich norm. Ponadto Komisja będzie zachęcać strony działające na rynku do opracowania odpowiednich otwartych specyfikacji w zakresie interoperacyjności. Komisja może – w drodze aktów delegowanych – nakazać stosowanie europejskich norm w zakresie interoperacyjności lub otwartych specyfikacji w zakresie interoperacyjności w przypadku określonych rodzajów usług poprzez odniesienie w centralnym repozytorium norm Unii dotyczące interoperacyjności usług przetwarzania danych. Normy europejskie i otwarte specyfikacje w zakresie interoperacyjności będą przywoływane wyłącznie wtedy, gdy będą zgodne z kryteriami określonymi w niniejszym rozporządzeniu, które mają takie samo znaczenie jak wymogi określone w pkt 3 i 4 załącznika II do rozporządzenia (UE) nr 1025/2021 oraz aspekty interoperacyjności określone w normie ISO/IEC 19941:2017.

(77) 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 dostępu władz 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 wzywającym państwem trzecim a Unią lub państwem członkowskim. W innych przypadkach mogą wystąpić sytuacje, w których wniosek o przekazanie danych nieosobowych lub udzielenie dostępu do nich wynikający z prawa państwa trzeciego pozostaje w sprzeczności z obowiązkiem ochrony takich

[67] 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).

danych wynikającym z prawa Unii lub prawa krajowego, w szczególności w odniesieniu do ochrony praw podstawowych osoby fizycznej, takich jak prawo do bezpieczeństwa i prawo do skutecznego środka prawnego, lub podstawowych interesów państwa członkowskiego związanych z bezpieczeństwem narodowym lub obroną, jak również z ochroną szczególnie chronionych danych handlowych, w tym ochroną tajemnic przedsiębiorstwa, oraz ochroną praw własności intelektualnej, w tym z zobowiązaniami umownymi tego państwa dotyczącymi poufności zgodnie z tym prawem. W przypadku braku umów międzynarodowych regulujących takie kwestie przekazywanie lub dostęp powinny być dozwolone tylko 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 w państwie trzecim, który jest upoważniony do należytego uwzględnienia odpowiednich interesów prawnych dostawcy takich danych. Wszędzie tam, gdzie jest to możliwe na mocy warunków wniosku o udostępnienie danych złożonego przez organ państwa trzeciego, dostawca usług przetwarzania danych powinien mieć możliwość poinformowania klienta, którego dane są przedmiotem wniosku, w celu sprawdzenia, czy istnieje potencjalny konflikt takiego dostępu z przepisami unijnymi lub krajowymi, takimi jak przepisy dotyczące ochrony szczególnie chronionych danych handlowych, w tym ochrony tajemnic przedsiębiorstwa i praw własności intelektualnej oraz zobowiązań umownych dotyczących poufności.

(78) Aby zwiększyć zaufanie do danych, należy w miarę możliwości wdrożyć zabezpieczenia w odniesieniu do obywateli Unii, sektora publicznego i przedsiębiorstw zapewniające kontrolę nad ich danymi. Ponadto należy przestrzegać prawa, wartości i standardów Unii w zakresie (między innymi) bezpieczeństwa, ochrony danych i prywatności oraz ochrony konsumentów. Aby zapobiec bezprawnemu dostępowi do danych nieosobowych, dostawcy usług przetwarzania danych podlegających temu instrumentowi, takich jak usługi w chmurze i usługi przetwarzania brzegowego, powinni wprowadzić wszelkie rozsądne środki w celu uniemożliwienia dostępu do systemów, w których przechowywane są dane nieosobowe, w tym, w stosownych przypadkach, poprzez szyfrowanie danych, częste poddawanie się audytom, zweryfikowane przestrzeganie odpowiednich systemów certyfikacji gwarancji bezpieczeństwa oraz zmianę polityki korporacyjnej.

(79) Kluczową rolę w dostarczaniu rozwiązań technicznych zapewniających interoperacyjność powinny odgrywać normalizacja i interoperacyjność semantyczna. W celu ułatwienia zgodności z wymogami interoperacyjności należy przewidzieć domniemanie zgodności rozwiązań interoperacyjnych spełniających normy zharmonizowane lub ich części zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012. Aby jeszcze bardziej zwiększyć interoperacyjność wspólnych europejskich przestrzeni danych, interfejsów programowania aplikacji, zmiany dostawcy usług w chmurze oraz inteligentnych umów, Komisja powinna przyjąć wspólne specyfikacje w obszarach, w których nie istnieją normy zharmonizowane lub w których są one niewystarczające. Ponadto nadal można byłoby przyjmować wspólne specyfikacje w poszczególnych sektorach zgodnie z unijnym lub krajowym prawem sektorowym, z uwzględnieniem szczególnych potrzeb tych sektorów. Część specyfikacji technicznych w zakresie interoperacyjności semantycznej powinny również stanowić struktury i modele danych wielokrotnego użytku (w formie podstawowych słowników), ontologie, profil aplikacji metadanych, dane referencyjne w formie podstawowych słowników, taksonomie, wykazy kodów, tabele uprawnień oraz tezaurusy. Ponadto Komisja powinna mieć możliwość zlecenia

opracowania norm zharmonizowanych w zakresie interoperacyjności usług przetwarzania danych.

(80) Aby promować interoperacyjność inteligentnych umów w aplikacjach do udostępniania danych, należy określić zasadnicze wymagania dotyczące inteligentnych umów dla specjalistów, którzy tworzą inteligentne umowy dla innych osób lub włączają takie inteligentne umowy do aplikacji wspierających realizację umów na potrzeby udostępniania danych. Aby ułatwić zgodność takich inteligentnych umów z tymi zasadniczymi wymaganiami, należy przewidzieć domniemanie zgodności inteligentnych umów spełniających normy zharmonizowane lub ich części zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012.

(81) Aby zapewnić skuteczne wdrożenie niniejszego rozporządzenia, państwa członkowskie powinny wyznaczyć co najmniej jeden właściwy organ. Jeżeli państwo członkowskie wyznacza więcej niż jeden właściwy organ, powinno również wyznaczyć właściwy organ koordynujący. Właściwe organy powinny ze sobą współpracować. Organy odpowiedzialne za nadzór nad przestrzeganiem przepisów dotyczących ochrony danych oraz właściwe organy wyznaczone na podstawie przepisów sektorowych powinny być odpowiedzialne za stosowanie niniejszego rozporządzenia w obszarach swoich kompetencji.

(82) 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 do właściwych organów. Organy te powinny być zobowiązane do współpracy w celu zapewnienia właściwego rozpatrzenia i rozstrzygnięcia skargi. Aby wykorzystać mechanizm sieci współpracy w zakresie ochrony konsumentów i umożliwić występowanie z powództwem przedstawicielskim, niniejsze rozporządzenie zmienia załączniki do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2394[68] oraz do dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/1828[69].

(83) Właściwe organy państw członkowskich powinny zapewnić, aby naruszenia obowiązków określonych w niniejszym rozporządzeniu podlegały karom. W tym celu powinny wziąć pod uwagę charakter, wagę, powtarzalność i czas trwania naruszenia, mając na uwadze określony interes publiczny, zakres i rodzaj prowadzonej działalności, jak również możliwości ekonomiczne sprawcy naruszenia. Powinny one uwzględnić, czy sprawca naruszenia systematycznie lub w sposób powtarzający się nie wypełnia swoich obowiązków wynikających z niniejszego rozporządzenia. Aby pomóc przedsiębiorstwom w opracowywaniu i negocjowaniu umów, Komisja powinna opracować i zalecić nieobowiązkowe modelowe postanowienia umowne na potrzeby umów dotyczących udostępniania danych między przedsiębiorstwami, w razie potrzeby z uwzględnieniem warunków panujących w poszczególnych sektorach i istniejących praktyk w zakresie mechanizmów dobrowolnego udostępniania danych. Te modelowe postanowienia umowne powinny być przede

---

68 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).

69 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).

wszystkim praktycznym narzędziem pomagającym zwłaszcza mniejszym przedsiębiorstwom w zawarciu umowy. Jeżeli te modelowe postanowienia umowne będą stosowane powszechnie i w całości, powinny mieć również korzystny wpływ na kształt umów dotyczących dostępu do danych i korzystania z nich, a tym samym prowadzić w szerszym ujęciu do bardziej sprawiedliwych stosunków umownych przy dostępie do danych i ich udostępnianiu.

(84) Aby wyeliminować ryzyko, że posiadacze danych w bazach danych uzyskanych lub wygenerowanych za pomocą elementów fizycznych, takich jak czujniki, produktu skomunikowanego i powiązanej usługi będą powoływać się na prawo *sui generis* określone w art. 7 dyrektywy 96/9/WE, w przypadku gdy takie bazy danych nie kwalifikują się do prawa *sui generis*, a tym samym będą ograniczać skuteczne wykonywanie prawa użytkowników do dostępu do danych i korzystania z nich oraz prawa do udostępniania danych osobom trzecim na podstawie niniejszego rozporządzenia, w niniejszym rozporządzeniu należy wyjaśnić, że prawo *sui generis* nie ma zastosowania do takich baz danych, ponieważ wymogi ochrony nie zostałyby spełnione.

(85) Aby uwzględnić aspekty techniczne 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, doprecyzowania zasadniczych wymagań w zakresie interoperacyjności dla operatorów przestrzeni danych i dostawców usług przetwarzania danych oraz opublikowania odniesień do otwartych specyfikacji w zakresie interoperacyjności i norm europejskich w zakresie interoperacyjności usług przetwarzania danych. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[70]. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(86) Aby zapewnić jednolite warunki wykonywania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do uzupełnienia niniejszego rozporządzenia w celu przyjęcia wspólnych specyfikacji służących zapewnieniu interoperacyjności wspólnych europejskich przestrzeni danych i udostępniania danych, zmiany dostawcy usług przetwarzania danych, interoperacyjności inteligentnych umów, a także środków technicznych, takich jak interfejsy programowania aplikacji, umożliwiających przekazywanie danych między stronami, w tym w sposób ciągły lub w czasie rzeczywistym, oraz podstawowych słowników interoperacyjności semantycznej, jak również w celu przyjęcia wspólnych specyfikacji dotyczących inteligentnych umów. Uprawnienia te powinny być

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

wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[71].

(87) Niniejsze rozporządzenie nie powinno mieć wpływu na przepisy szczegółowe aktów prawnych Unii przyjętych w dziedzinie udostępniania danych między przedsiębiorstwami, między przedsiębiorstwami a konsumentami oraz między przedsiębiorstwami a organami sektora publicznego, które to akty prawne przyjęto przed przyjęciem niniejszego rozporządzenia. W celu zapewnienia spójności i sprawnego funkcjonowania rynku wewnętrznego Komisja powinna, w stosownych przypadkach, ocenić sytuację w odniesieniu do związku między niniejszym rozporządzeniem a regulującymi udostępnianie danych aktami przyjętymi przed przyjęciem niniejszego rozporządzenia, tak aby ocenić potrzebę dostosowania tych przepisów szczegółowych do niniejszego rozporządzenia. Niniejsze rozporządzenie nie powinno naruszać przepisów dotyczących potrzeb specyficznych dla poszczególnych sektorów lub obszarów służących interesowi publicznemu. Przepisy takie mogą obejmować dodatkowe wymogi dotyczące aspektów technicznych dostępu do danych, takich jak interfejsy dostępu do danych, lub sposobu zapewniania dostępu do danych, na przykład bezpośrednio z produktu lub poprzez usługi pośrednictwa w zakresie danych. Przepisy takie mogą również obejmować ograniczenia praw posiadaczy danych do dostępu do danych użytkowników lub do korzystania z nich, lub inne aspekty wykraczające poza dostęp do danych i korzystanie z nich, takie jak aspekty zarządzania. Niniejsze rozporządzenie nie powinno również naruszać bardziej szczegółowych przepisów w kontekście rozwoju wspólnych europejskich przestrzeni danych.

(88) Niniejsze rozporządzenie nie powinno wpływać na stosowanie reguł konkurencji, w szczególności art. 101 i 102 Traktatu. Środków przewidzianych w niniejszym rozporządzeniu nie należy stosować do ograniczania konkurencji w sposób sprzeczny z Traktatem.

(89) Aby umożliwić podmiotom gospodarczym dostosowanie się do nowych przepisów określonych w niniejszym rozporządzeniu, przepisy te powinny zacząć obowiązywać po roku od wejścia rozporządzenia w życie.

(90) Zgodnie z art. 42 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, którzy wydali wspólną opinię dnia [XX XX 2022 r.],

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i zakres stosowania

1. W niniejszym rozporządzeniu ustanawia się zharmonizowane przepisy dotyczące udostępniania danych generowanych w wyniku korzystania z produktu lub powiązanej usługi użytkownikom tego produktu lub tej usługi, udostępniania danych

[71] 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).

przez posiadaczy danych odbiorcom danych oraz udostępniania danych przez posiadaczy danych organom sektora publicznego lub instytucjom, agencjom lub organom Unii, w przypadku wystąpienia wyjątkowej potrzeby, do celów wykonania zadania realizowanego w interesie publicznym:

2. Niniejsze rozporządzenie ma zastosowanie do:

   a) producentów produktów i dostawców powiązanych usług wprowadzanych do obrotu w Unii oraz użytkowników takich produktów lub usług;

   b) posiadaczy danych, którzy udostępniają dane odbiorcom danych w Unii;

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

   d) organów sektora publicznego oraz instytucji, agencji lub organów Unii, które w przypadku wystąpienia wyjątkowej potrzeby zwracają się do posiadaczy danych z wnioskiem o udostępnienie tych danych do celów wykonania zadania realizowanego w interesie publicznym, oraz posiadaczy danych, którzy przekazują te dane w odpowiedzi na taki wniosek;

   e) dostawców usług przetwarzania danych oferujących takie usługi klientom w Unii.

3. Do danych osobowych przetwarzanych w związku z prawami i obowiązkami określonymi w niniejszym rozporządzeniu zastosowanie ma prawo Unii dotyczące ochrony danych osobowych, prywatności i poufności komunikacji oraz integralności urządzeń końcowych. Niniejsze rozporządzenie nie ma wpływu na stosowanie prawa Unii dotyczącego ochrony danych osobowych, w szczególności rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, w tym na uprawnienia i kompetencje organów nadzorczych. W zakresie, w jakim dotyczy to praw określonych w rozdziale II niniejszego rozporządzenia, oraz w przypadku gdy użytkownicy są osobami, których dane osobowe dotyczą, podlegającymi prawom i obowiązkom wynikającym z tego rozdziału, przepisy niniejszego rozporządzenia uzupełniają prawo do przenoszenia danych określone w art. 20 rozporządzenia (UE) 2016/679.

4. Niniejsze rozporządzenie nie ma wpływu na unijne i krajowe akty prawne przewidujące wymianę danych, dostęp do nich i ich wykorzystywanie do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar, w tym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784[72] i [wnioski dotyczące elektronicznego materiału dowodowego [COM(2018) 225 i COM(2018) 226] po ich przyjęciu ani na współpracę międzynarodową w tej dziedzinie. Niniejsze rozporządzenie nie ma wpływu na gromadzenie i wymianę danych, dostęp do danych i ich wykorzystywanie na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/847 w sprawie informacji towarzyszących transferom środków pieniężnych. Niniejsze rozporządzenie nie ma wpływu na kompetencje państw członkowskich w odniesieniu do działań związanych z bezpieczeństwem publicznym, obroną, bezpieczeństwem narodowym, administracją celną i podatkową oraz zdrowiem i bezpieczeństwem obywateli zgodnie z prawem Unii.

[72] 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).

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) „produkt” oznacza materialną rzecz ruchomą, w tym zawartą w rzeczy nieruchomej, która pozyskuje, generuje lub gromadzi dane dotyczące jej wykorzystania lub środowiska, która jest w stanie przekazywać dane za pośrednictwem publicznie dostępnych usług łączności elektronicznej i której podstawową funkcją nie jest przechowywanie ani przetwarzanie danych;

3) „powiązana usługa” oznacza usługę cyfrową, w tym oprogramowanie, która jest zawarta w produkcie lub wzajemnie z nim połączona w taki sposób, że jej brak uniemożliwiłby produktowi wykonywanie jednej z jego funkcji;

4) „wirtualni asystenci” oznaczają oprogramowanie, które może przetwarzać żądania, zadania lub pytania, w tym na podstawie dźwięku, pisma, gestów lub ruchów, oraz w oparciu o te żądania, zadania lub pytania zapewnia dostęp do usług własnych i usług osób trzecich lub kontroluje urządzenia własne i urządzenia osób trzecich;

5) „użytkownik” oznacza osobę fizyczną lub prawną, która posiada lub wynajmuje produkt, korzysta z produktu na zasadzie leasingu lub otrzymuje usługi;

6) „posiadacz danych” oznacza osobę prawną lub fizyczną, która ma prawo lub obowiązek, zgodnie z niniejszym rozporządzeniem, mającym zastosowanie prawem Unii lub przepisami krajowymi wdrażającymi prawo Unii, udostępniać określone dane lub – w przypadku danych nieosobowych i poprzez kontrolę technicznego projektu produktu i powiązanych usług – ma zdolność do udostępniania określonych danych;

7) „odbiorca danych” oznacza osobę prawną lub fizyczną działającą w celach związanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, inną niż użytkownik produktu lub powiązanej usługi, 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 przepisów krajowych wdrażających prawo Unii;

8) „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;

9) „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;

10) „niebezpieczeństwo publiczne” oznacza wyjątkową sytuację negatywnie wpływającą na ludność Unii, państwa członkowskiego lub jego części, która to sytuacja wiąże się z ryzykiem wystąpienia poważnych i trwałych następstw dla warunków życia lub stabilności gospodarczej, lub znacznego obniżenia wartości aktywów gospodarczych w Unii lub w odpowiednim państwie członkowskim;

11) „przetwarzanie” oznacza każdą operację lub zestaw operacji wykonywanych na danych lub zbiorach danych w formie elektronicznej w sposób zautomatyzowany lub niezautomatyzowany, takie jak gromadzenie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

12) „usługa przetwarzania danych” oznacza usługę cyfrową inną niż usługa online w zakresie treści zdefiniowana w art. 2 pkt 5 rozporządzenia (UE) 2017/1128, świadczoną klientowi, która umożliwia administrowanie na żądanie skalowalnym i elastycznym zbiorem scentralizowanych, rozproszonych lub wysoce rozproszonych zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru;

13) „rodzaj usługi” oznacza zestaw usług przetwarzania danych, które mają ten sam główny cel i ten sam podstawowy model usługi przetwarzania danych;

14) „równoważność funkcjonalna” oznacza zachowanie minimalnego poziomu funkcjonalności w środowisku nowej usługi przetwarzania danych po procesie zmiany dostawcy w takim stopniu, że w odpowiedzi na działanie wejściowe użytkownika w podstawowych elementach usługi usługa docelowa dostarczy taki sam rezultat wyjściowy przy takiej samej wydajności i takim samym poziomie bezpieczeństwa, odporności operacyjnej i jakości usługi jak usługa pierwotna w momencie rozwiązania umowy;

15) „otwarte specyfikacje w zakresie interoperacyjności” oznaczają specyfikacje techniczne ICT zdefiniowane w rozporządzeniu (UE) nr 1025/2012, które są ukierunkowane na osiągnięcie interoperacyjności między usługami przetwarzania danych;

16) „inteligentna umowa” oznacza program komputerowy przechowywany w systemie rejestru elektronicznego, w którym to systemie wynik wykonania programu jest zapisywany w rejestrze elektronicznym;

17) „rejestr elektroniczny” oznacza rejestr elektroniczny w rozumieniu art. 3 pkt 53 rozporządzenia (UE) nr 910/2014;

18) „wspólne specyfikacje” oznaczają dokument inny niż norma, zawierający rozwiązania techniczne zapewniające środki umożliwiające spełnienie niektórych wymogów i obowiązków ustanowionych na mocy niniejszego rozporządzenia;

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

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

ROZDZIAŁ II
UDOSTĘPNIANIE DANYCH PRZEZ PRZEDSIĘBIORSTWA KONSUMENTOM I MIĘDZY PRZEDSIĘBIORSTWAMI

Artykuł 3

Obowiązek udostępniania danych generowanych w wyniku korzystania z produktów lub powiązanych usług

1. Produkty muszą być projektowane i wytwarzane, a powiązane usługi świadczone w taki sposób, aby dane generowane w wyniku korzystania z nich były domyślnie łatwo, bezpiecznie oraz, w razie potrzeby i w stosownych przypadkach, bezpośrednio dostępne dla użytkownika.

2. Przed zawarciem umowy dotyczącej zakupu, najmu lub leasingu produktu lub świadczenia powiązanej usługi użytkownik musi otrzymać co najmniej następujące informacje w jasnym i zrozumiałym formacie:

   a) charakter i ilość danych, które mogą być generowane w wyniku korzystania z produktu lub powiązanej usługi;

   b) czy istnieje prawdopodobieństwo, że dane będą generowane w sposób ciągły i w czasie rzeczywistym;

   c) w jaki sposób użytkownik może uzyskać dostęp do tych danych;

   d) czy producent dostarczający produkt lub dostawca powiązanej usługi zamierza sam wykorzystywać dane lub zezwolić na ich wykorzystywanie osobie trzeciej, a jeżeli tak, to do jakich celów dane te będą wykorzystywane;

   e) czy sprzedawca, oddający w najem lub leasingodawca jest posiadaczem danych, a jeżeli nie, jaka jest tożsamość posiadacza danych, np. jego nazwa handlowa i adres geograficzny, pod którym ma siedzibę;

   f) środki komunikacji umożliwiające użytkownikowi szybki kontakt z posiadaczem danych i sprawną komunikację z nim;

   g) w jaki sposób użytkownik może zażądać udostępnienia danych osobie trzeciej;

   h) prawo użytkownika do wniesienia skargi dotyczącej naruszenia przepisów niniejszego rozdziału do właściwego organu, o którym mowa w art. 31.

Artykuł 4

Prawo użytkowników do dostępu do danych generowanych w wyniku korzystania z produktów lub powiązanych usług oraz do korzystania z tych danych

1. Jeżeli użytkownik nie może uzyskać bezpośredniego dostępu do danych z produktu, posiadacz danych udostępnia użytkownikowi – bez zbędnej zwłoki, nieodpłatnie oraz, w stosownych przypadkach, w sposób ciągły i w czasie rzeczywistym – dane wygenerowane w wyniku korzystania przez niego z produktu lub powiązanej usługi. Odbywa się to na podstawie zwykłego wniosku złożonego drogą elektroniczną, jeżeli jest to technicznie wykonalne.

2. Posiadacz danych nie wymaga od użytkownika podawania żadnych informacji poza tymi, które są konieczne do zweryfikowania, czy jest on użytkownikiem zgodnie z ust. 1. Posiadacz danych nie może przechowywać żadnych informacji na temat dostępu użytkownika do żądanych danych poza informacjami, które są niezbędne do

należytego wykonania wniosku użytkownika o uzyskanie dostępu oraz do bezpieczeństwa i utrzymania infrastruktury danych.

3. Tajemnice przedsiębiorstwa ujawnia się wyłącznie pod warunkiem zastosowania wszelkich szczególnych środków niezbędnych do zachowania poufności tajemnic przedsiębiorstwa, w szczególności w odniesieniu do osób trzecich. Posiadacz danych i użytkownik mogą uzgodnić środki mające na celu zachowanie poufności udostępnianych danych, w szczególności w odniesieniu do osób trzecich.

4. Użytkownik nie może wykorzystywać danych uzyskanych na podstawie wniosku, o którym mowa w ust. 1, do opracowania produktu konkurującego z produktem, z którego pochodzą dane.

5. Jeżeli użytkownik nie jest osobą, której dane dotyczą, wszelkie dane osobowe wygenerowane w wyniku korzystania z produktu lub powiązanej usługi są udostępniane użytkownikowi przez posiadacza danych wyłącznie wtedy, gdy istnieje ważna podstawa prawna zgodnie z art. 6 ust. 1 rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, spełnione są warunki określone w art. 9 rozporządzenia (UE) 2016/679.

6. Posiadacz danych wykorzystuje wszelkie dane nieosobowe wygenerowane w wyniku korzystania z produktu lub powiązanej usługi wyłącznie na podstawie umowy z użytkownikiem. Posiadacz danych nie może wykorzystywać takich danych wygenerowanych w wyniku korzystania z produktu lub powiązanej usługi do pozyskania informacji na temat sytuacji ekonomicznej, aktywów i metod produkcji użytkownika lub korzystania przez użytkownika, które to informacje mogłyby osłabić pozycję handlową użytkownika na rynkach, na których prowadzi on działalność.

Artykuł 5
Prawo do udostępniania danych osobom trzecim

1. Na wniosek użytkownika lub strony działającej w jego imieniu posiadacz danych udostępnia osobie trzeciej – bez zbędnej zwłoki, nieodpłatnie oraz, w stosownych przypadkach, w sposób ciągły i w czasie rzeczywistym – dane wygenerowane w wyniku korzystania z produktu lub powiązanej usługi cechujące się taką samą jakością, jaka jest dostępna posiadaczowi danych.

2. Żadne przedsiębiorstwo świadczące podstawowe usługi platformowe, w przypadku którego co najmniej jedną z takich usług wyznaczono jako strażnika dostępu na podstawie art. [...] [rozporządzenia XXX w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych)[73]], nie może być kwalifikującą się osobą trzecią na mocy niniejszego artykułu, a zatem nie może:

   a) nakłaniać ani komercyjnie zachęcać użytkownika w żaden sposób, w tym przez zapewnienie wynagrodzenia pieniężnego lub jakiegokolwiek innego, do udostępnienia danych, które użytkownik uzyskał na podstawie wniosku złożonego zgodnie z art. 4 ust. 1, na potrzeby jednej ze swoich usług;

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

[73] Dz.U. […].

c) otrzymywać danych od użytkownika, które użytkownik uzyskał na podstawie wniosku złożonego zgodnie z art. 4 ust. 1.

3. Użytkownik lub osoba trzecia nie są zobowiązani do podawania żadnych informacji poza tymi, które są konieczne do zweryfikowania, czy są oni użytkownikiem lub osobą trzecią zgodnie z ust. 1. Posiadacz danych nie może przechowywać żadnych informacji na temat dostępu osoby trzeciej do żądanych danych poza informacjami, które są niezbędne do należytego wykonania wniosku osoby trzeciej o uzyskanie dostępu oraz do bezpieczeństwa i utrzymania infrastruktury danych.

4. Osoba trzecia nie może stosować środków przymusu ani nadużywać oczywistych luk w infrastrukturze technicznej posiadacza danych, która ma chronić dane, w celu uzyskania dostępu do danych.

5. Posiadacz danych nie może wykorzystywać żadnych danych nieosobowych wygenerowanych w wyniku korzystania z produktu lub powiązanej usługi do pozyskania informacji na temat sytuacji ekonomicznej, aktywów i metod produkcji osoby trzeciej lub korzystania przez osobę trzecią, które to informacje mogłyby osłabić pozycję handlową osoby trzeciej na rynkach, na których prowadzi ona działalność, chyba że osoba trzecia wyraziła zgodę na takie wykorzystanie i ma techniczną możliwość wycofania tej zgody w dowolnym momencie.

6. Jeżeli użytkownik nie jest osobą, której dane dotyczą, wszelkie dane osobowe wygenerowane w wyniku korzystania z produktu lub powiązanej usługi są udostępniane wyłącznie wtedy, gdy istnieje ważna podstawa prawna zgodnie z art. 6 ust. 1 rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, spełnione są warunki określone w art. 9 rozporządzenia (UE) 2016/679.

7. Wszelkie przypadki nieuzgodnienia przez posiadacza danych i osobę trzecią ustaleń dotyczących przekazywania danych nie mogą utrudniać, uniemożliwiać ani zakłócać wykonywania praw przysługujących osobie, której dane dotyczą, na podstawie rozporządzenia (UE) 2016/679, a w szczególności prawa do przenoszenia danych określonego w art. 20 tego rozporządzenia.

8. Tajemnice przedsiębiorstwa ujawnia się osobom trzecim wyłącznie w zakresie, w jakim są one absolutnie niezbędne do osiągnięcia celu uzgodnionego między użytkownikiem a osobą trzecią, a osoba trzecia stosuje wszystkie szczególne niezbędne środki uzgodnione między posiadaczem danych a osobą trzecią w celu zachowania poufności tajemnicy przedsiębiorstwa. W takim przypadku charakter danych jako tajemnic przedsiębiorstwa oraz środki służące zachowaniu poufności określa się w umowie między posiadaczem danych a osobą trzecią.

9. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa innych osób do ochrony danych.

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 z zastrzeżeniem praw osoby, której dane dotyczą, w odniesieniu do danych osobowych, oraz usuwa dane, gdy nie są już one niezbędne do uzgodnionego celu.

2. Osoba trzecia nie może:

a) w żaden sposób zmuszać ani oszukiwać użytkownika ani też nim manipulować poprzez podważenie lub ograniczenie autonomii, zdolności decyzyjnej lub wyborów użytkownika, w tym za pomocą interfejsu cyfrowego z użytkownikiem;

b) wykorzystywać otrzymanych danych do profilowania osób fizycznych w rozumieniu art. 4 pkt 4 rozporządzenia (UE) 2016/679, chyba że jest to konieczne do świadczenia usługi zażądanej przez użytkownika;

c) udostępniać otrzymanych danych innej osobie trzeciej w formie surowej, zagregowanej lub pochodnej, chyba że jest to konieczne do świadczenia usługi zażądanej przez użytkownika;

d) udostępniać otrzymanych danych przedsiębiorstwu świadczącemu podstawowe usługi platformowe, w przypadku którego co najmniej jedną z takich usług wyznaczono jako strażnika dostępu na podstawie art. [...] [rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych)];

e) wykorzystywać otrzymanych danych do opracowania produktu konkurującego z produktem, z którego pochodzą dane, do których uzyskano dostęp, ani udostępniać ich w tym celu innej osobie trzeciej;

f) uniemożliwiać użytkownikowi, w tym w drodze zobowiązań umownych, udostępniania innym osobom otrzymanych przez siebie danych.

Artykuł 7

Zakres obowiązków udostępniania danych przez przedsiębiorstwa konsumentom i między przedsiębiorstwami

1. Obowiązki określone w niniejszym rozdziale nie mają zastosowania do danych generowanych w wyniku korzystania z wytworzonych produktów lub powiązanych usług dostarczonych przez przedsiębiorstwa, które kwalifikują się jako mikroprzedsiębiorstwa lub małe przedsiębiorstwa zgodnie z definicją w art. 2 załącznika do zalecenia 2003/361/WE, pod warunkiem że przedsiębiorstwa te nie mają przedsiębiorstw partnerskich ani przedsiębiorstw powiązanych zdefiniowanych w art. 3 załącznika do zalecenia 2003/361/WE, które nie kwalifikują się jako mikroprzedsiębiorstwa lub małe przedsiębiorstwa.

2. W przypadku gdy w niniejszym rozporządzeniu mowa jest o produktach lub powiązanych usługach, takie odniesienie rozumie się jako obejmujące również wirtualnych asystentów, o ile są oni wykorzystywani do uzyskiwania dostępu do produktu lub powiązanej usługi lub sterowania nimi.

ROZDZIAŁ III
OBOWIĄZKI POSIADACZY DANYCH PRAWNIE ZOBOWIĄZANYCH DO UDOSTĘPNIANIA DANYCH

Artykuł 8

Warunki, na jakich posiadacze danych udostępniają dane odbiorcom danych

1. W przypadku gdy posiadacz danych jest zobowiązany do udostępniania danych odbiorcy danych na podstawie art. 5 lub innych przepisów prawa Unii, lub przepisów krajowych wdrażających prawo Unii, musi czynić to na sprawiedliwych, rozsądnych

i niedyskryminujących warunkach oraz w przejrzysty sposób zgodnie z przepisami niniejszego rozdziału i rozdziału IV.

2. Posiadacz danych uzgadnia z odbiorcą danych warunki udostępniania danych. Postanowienie umowne dotyczące dostępu do danych i korzystania z nich lub odpowiedzialności i środków ochrony prawnej w zakresie naruszenia lub wygaśnięcia obowiązków dotyczących danych nie jest wiążące, jeżeli spełnia warunki określone w art. 13 lub jeżeli wyłącza stosowanie skutków praw użytkownika wynikających z rozdziału II, stanowi odstępstwo od tych skutków lub je zmienia.

3. Przy udostępnianiu danych posiadacz danych nie wprowadza rozróżnienia między porównywalnymi kategoriami odbiorców danych, w tym przedsiębiorstwami partnerskimi lub przedsiębiorstwami powiązanymi posiadacza danych zdefiniowanymi w art. 3 załącznika do zalecenia 2003/361/WE. W przypadku gdy odbiorca danych uważa, że warunki, na jakich dane zostały mu udostępnione, są dyskryminujące, to do posiadacza danych należy wykazanie, że nie doszło do dyskryminacji.

4. Posiadacz danych nie udostępnia danych odbiorcy danych na zasadzie wyłączności, chyba że użytkownik zażąda tego na podstawie rozdziału II.

5. Posiadacze danych i odbiorcy danych nie są zobowiązani do podawania żadnych informacji poza tymi, które są konieczne do weryfikacji zgodności z postanowieniami umownymi uzgodnionymi w celu udostępniania danych lub z ich obowiązkami wynikającymi z niniejszego rozporządzenia lub innych mających zastosowanie przepisów prawa Unii, lub przepisów krajowych wdrażających prawo Unii.

6. O ile prawo Unii, w tym art. 6 niniejszego rozporządzenia, lub przepisy krajowe wdrażające prawo Unii nie stanowią inaczej, obowiązek udostępniania danych odbiorcy danych nie zobowiązuje do ujawnienia tajemnic przedsiębiorstwa w rozumieniu dyrektywy (UE) 2016/943.

Artykuł 9
Wynagrodzenie za udostępnienie danych

1. Wszelkie wynagrodzenie uzgodnione między posiadaczem danych a odbiorcą danych za udostępnienie danych musi być rozsądne.

2. W przypadku gdy odbiorcą danych jest mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo w rozumieniu art. 2 załącznika do zalecenia 2003/361/WE, wszelkie uzgodnione wynagrodzenie nie może przekraczać kosztów, które są bezpośrednio związane z udostępnieniem danych odbiorcy danych i które można przypisać danemu wnioskowi. Art. 8 ust. 3 stosuje się odpowiednio.

3. Niniejszy artykuł nie stoi na przeszkodzie temu, by inne przepisy prawa Unii lub przepisy krajowe wdrażające prawo Unii wykluczały wynagrodzenie za udostępnienie danych lub przewidywały niższe wynagrodzenie.

4. Posiadacz danych przekazuje odbiorcy danych informacje określające podstawę obliczenia wynagrodzenia w sposób wystarczająco szczegółowy, tak aby odbiorca danych mógł zweryfikować, czy spełnione są wymogi określone w ust. 1 oraz, w stosownych przypadkach, w ust. 2.

Artykuł 10
Rozstrzyganie sporów

1. Posiadacze danych i odbiorcy danych mają dostęp do organów rozstrzygania sporów, certyfikowanych zgodnie z ust. 2 niniejszego artykułu, na potrzeby rozstrzygania sporów dotyczących ustalania sprawiedliwych, rozsądnych i niedyskryminujących warunków udostępniania danych oraz przejrzystego sposobu udostępniania danych zgodnie z art. 8 i 9.

2. Państwo członkowskie, w którym znajduje się siedziba organu rozstrzygania sporów, na wniosek tego organu dokonuje jego certyfikacji, jeżeli organ ten wykazał, że spełnia wszystkie następujące warunki:

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

   b) organ dysponuje niezbędną wiedzą ekspercką na temat ustalania sprawiedliwych, rozsądnych i niedyskryminujących warunków udostępniania danych oraz przejrzystego sposobu udostępniania danych, która to wiedza pozwala organowi na skuteczne ustalanie tych warunków;

   c) organ jest łatwo dostępny za pośrednictwem technologii łączności elektronicznej;

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

   Jeżeli do dnia [data rozpoczęcia stosowania rozporządzenia] r. w danym państwie członkowskim nie zostanie certyfikowany żaden organ rozstrzygania sporów, to państwo członkowskie ustanawia i certyfikuje organ rozstrzygania sporów, który spełnia warunki określone w lit. a)–d) niniejszego ustępu.

3. Państwa członkowskie zgłaszają Komisji organy rozstrzygania sporów certyfikowane zgodnie z ust. 2. Komisja publikuje wykaz tych organów na specjalnej stronie internetowej i aktualizuje go.

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

5. 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.

6. Organy rozstrzygania sporów dają stronom możliwość wyrażenia, w rozsądnym terminie, swojego stanowiska w sprawach wniesionych przez te strony do tych organów. W tym kontekście organy rozstrzygania sporów przekazują tym stronom opinie drugiej strony oraz wszelkie oświadczenia ekspertów. Organy te zapewniają stronom możliwość ustosunkowania się do tych opinii i oświadczeń.

7. Organy rozstrzygania sporów wydają decyzję w skierowanych do nich sprawach nie później niż w ciągu 90 dni od złożeniu wniosku o wydanie decyzji. Decyzje te sporządza się na piśmie lub na trwałym nośniku i opatruje uzasadnieniem.

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

9. Niniejszy artykuł nie ma wpływu 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, aby zapobiec nieuprawnionemu dostępowi do danych i zapewnić zgodność z art. 5, 6, 9 i 10, a także z uzgodnionymi postanowieniami umownymi dotyczącymi udostępniania danych. Takie techniczne środki ochrony nie mogą być wykorzystywane jako środek ograniczający prawo użytkownika do skutecznego dostarczania danych osobom trzecim na podstawie art. 5 ani jakiekolwiek prawo osoby trzeciej wynikające z prawa Unii lub przepisów krajowych wdrażających prawo Unii, o których mowa w art. 8 ust. 1.

2. Odbiorca danych, który w celu uzyskania danych przekazał posiadaczowi danych niedokładne lub nieprawdziwe informacje, zastosował środki wprowadzające w błąd lub środki przymusu lub nadużył oczywistych luk w infrastrukturze technicznej posiadacza danych mającej chronić dane, wykorzystał udostępnione dane w niedozwolonych celach lub ujawnił te dane innej osobie bez zgody posiadacza danych, musi bez zbędnej zwłoki, o ile posiadacz danych lub użytkownik nie wyda innego polecenia:

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

   b) zaprzestać produkcji, oferowania, wprowadzania do obrotu lub wykorzystywania towarów, pochodnych danych lub usług wytworzonych na podstawie wiedzy uzyskanej dzięki takim danym lub przywozu, wywozu lub przechowywania do tych celów towarów naruszających prawo oraz zniszczyć wszelkie towary naruszające prawo.

3. Ust. 2 lit. b) nie ma zastosowania w żadnym z następujących przypadków:

   a) korzystanie z danych nie spowodowało poważnych szkód dla posiadacza danych;

   b) byłoby to nieproporcjonalne w świetle interesów posiadacza danych.

Artykuł 12

Zakres obowiązków posiadaczy danych prawnie zobowiązanych do udostępniania danych

1. Niniejszy rozdział ma zastosowanie, w przypadku gdy posiadacz danych jest zobowiązany na mocy art. 5 lub prawa Unii, lub przepisów krajowych wdrażających prawo Unii, do udostępniania danych odbiorcy danych.

2. Wszelkie postanowienia umowne zawarte w umowie o udostępnianiu danych, które ze szkodą dla jednej ze stron lub, w stosownych przypadkach, ze szkodą dla użytkownika wyłączają stosowanie niniejszego rozdziału, stanowią odstępstwo od niego lub zmieniają jego skutki, nie są wiążące dla tej strony.

3. Niniejszy rozdział ma zastosowanie wyłącznie do obowiązków udostępniania danych na podstawie przepisów prawa Unii lub przepisów krajowych wdrażających prawo Unii, które wchodzą w życie po dniu [data rozpoczęcia stosowania rozporządzenia] r.

ROZDZIAŁ IV
NIEUCZCIWE POSTANOWIENIA W UMOWACH MIĘDZY PRZEDSIĘBIORSTWAMI DOTYCZĄCE DOSTĘPU DO DANYCH I KORZYSTANIA Z NICH

Artykuł 13

Nieuczciwe postanowienia umowne jednostronnie nałożone na mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo

1. Postanowienie umowne dotyczące dostępu do danych i korzystania z nich lub odpowiedzialności i środków ochrony prawnej w zakresie naruszenia lub wygaśnięcia zobowiązań dotyczących danych, które przedsiębiorstwo jednostronnie nałożyło na mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo zdefiniowane w art. 2 załącznika do zalecenia 2003/361/WE, nie jest wiążące dla tego mikroprzedsiębiorstwa lub małego lub średniego przedsiębiorstwa, jeżeli postanowienie to jest nieuczciwe.

2. Postanowienie umowne jest nieuczciwe, jeżeli cechuje się tym, że jego stosowanie rażąco odbiega od dobrej praktyki handlowej w zakresie dostępu do danych i korzystania z nich, co jest sprzeczne z zasadą dobrej wiary i uczciwego obrotu.

3. Postanowienie umowne jest nieuczciwe do celów niniejszego artykułu, jeżeli jego celem lub skutkiem jest:

   a) wyłączenie lub ograniczenie odpowiedzialności strony, która jednostronnie nałożyła to postanowienie, za czyny umyślne lub rażące niedbalstwo;

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

   c) przyznanie stronie, która jednostronnie nałożyła to postanowienie umowne, wyłącznego prawa ustalania, czy dostarczone dane są zgodne z umową, lub wyłącznego prawa do interpretowania postanowień umowy.

4. Postanowienie umowne uznaje się za nieuczciwe do celów niniejszego artykułu, 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;

   b) umożliwienie stronie, która jednostronnie nałożyła to postanowienie, dostępu do danych drugiej umawiającej się strony i korzystania z nich w sposób znacząco szkodliwy dla uzasadnionych interesów drugiej umawiającej się strony;

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

d) uniemożliwienie stronie, na którą jednostronnie nałożono to postanowienie, uzyskania kopii danych przekazanych lub wygenerowanych przez tę stronę w okresie obowiązywania umowy lub w rozsądnym okresie po jej rozwiązaniu;

e) umożliwienie stronie, która jednostronnie nałożyła to postanowienie, rozwiązania umowy ze zbyt krótkim terminem wypowiedzenia, biorąc pod uwagę racjonalne możliwości drugiej umawiającej się strony w zakresie zmiany usługi na alternatywną i porównywalną usługę oraz szkodę finansową spowodowaną takim rozwiązaniem, chyba że istnieją ku temu poważne podstawy.

5. Postanowienie umowne uważa się za nałożone jednostronnie 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 prób negocjacji tej treści. Ciężar udowodnienia, że postanowienie umowne nie zostało nałożone jednostronnie, spoczywa na umawiającej się stronie, która zaproponowała to postanowienie.

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

7. Niniejszy artykuł nie ma zastosowania do postanowień umownych określających główny przedmiot umowy ani do postanowień umownych określających cenę do zapłaty.

8. Strony umowy objętej ust. 1 nie mogą wyłączyć stosowania niniejszego artykułu, odstąpić od niego ani zmienić jego skutków.

ROZDZIAŁ V
UDOSTĘPNIANIE DANYCH ORGANOM SEKTORA PUBLICZNEGO ORAZ INSTYTUCJOM, AGENCJOM LUB ORGANOM UNII W PRZYPADKU WYJĄTKOWEJ POTRZEBY

Artykuł 14
Obowiązek udostępniania danych w przypadku wyjątkowej potrzeby

1. Posiadacz danych na wniosek udostępnia dane organowi sektora publicznego lub instytucji, agencji lub organowi Unii wykazującym wyjątkową potrzebę skorzystania z żądanych danych.

2. Niniejszy rozdział nie ma zastosowania do małych przedsiębiorstw i mikroprzedsiębiorstw zdefiniowanych w art. 2 załącznika do zalecenia 2003/361/WE.

Artykuł 15
Wyjątkowa potrzeba skorzystania z danych

Uznaje się, że wyjątkowa potrzeba skorzystania z danych w rozumieniu niniejszego rozdziału istnieje w następujących okolicznościach:

a) gdy żądane dane są niezbędne do zareagowania na niebezpieczeństwo publiczne;

b) gdy wniosek o udostępnienie danych jest ograniczony w czasie i zakresie oraz niezbędny do zapobieżenia niebezpieczeństwu publicznemu lub do pomocy w przywracaniu stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego;

c) gdy brak dostępnych danych uniemożliwia organowi sektora publicznego lub instytucji, agencji lub organowi Unii realizację konkretnego zadania leżącego w interesie publicznym i wyraźnie wskazanego w prawie; oraz

1) organ sektora publicznego lub instytucja, agencja lub organ Unii nie były w stanie uzyskać takich danych za pomocą alternatywnych środków, w tym w drodze zakupu danych na rynku po stawkach rynkowych lub poprzez poleganie na istniejących obowiązkach udostępniania danych, a przyjęcie nowych środków ustawodawczych nie może zapewnić terminowej dostępności danych; lub

2) uzyskanie danych zgodnie z procedurą określoną w niniejszym rozdziale znacznie zmniejszyłoby obciążenie administracyjne posiadaczy danych lub innych przedsiębiorstw.

Artykuł 16
Związek z innymi obowiązkami udostępniania danych organom sektora publicznego oraz instytucjom, agencjom i organom Unii

1. Niniejszy rozdział nie ma wpływu na obowiązki określone w prawie Unii lub prawie krajowym do celów sprawozdawczości, stosowania się do wniosków o udzielenie informacji lub wykazywania lub weryfikowania zgodności z zobowiązaniami prawnymi.

2. Prawa wynikające z niniejszego rozdziału nie mogą być wykonywane przez organy sektora publicznego ani instytucje, agencje i organy Unii w celu prowadzenia działań w zakresie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych lub wykonywania kar ani działań na potrzeby administracji celnej lub podatkowej. Niniejszy rozdział nie ma wpływu na mające zastosowanie prawo unijne i 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 udostępnienie danych na podstawie art. 14 ust. 1, organ sektora publicznego lub instytucja, agencja lub organ Unii musi:

a) określić, o udostępnienie jakich danych się wnioskuje;

b) wykazać wyjątkową potrzebę, z powodu której wnioskuje się o udostępnienie danych;

c) wyjaśnić cel wniosku, planowane wykorzystanie żądanych danych oraz czas trwania tego wykorzystywania;

d) podać podstawę prawną występowania z wnioskiem o udostępnienie danych;

e) określić termin, w którym dane mają zostać udostępnione lub w którym posiadacz danych może zwrócić się do organu sektora publicznego lub do instytucji, agencji lub organu Unii o zmianę lub wycofanie wniosku.

2. Wniosek o udostępnienie danych złożony na podstawie ust. 1 niniejszego artykułu musi:

a) być sformułowany jasnym, zwięzłym i prostym językiem zrozumiałym dla posiadacza danych;

b) być proporcjonalny do wyjątkowej potrzeby pod względem szczegółowości i ilości żądanych danych oraz częstotliwości dostępu do żądanych danych;

c) respektować prawnie uzasadnione cele posiadacza danych, biorąc pod uwagę ochronę tajemnic przedsiębiorstwa oraz koszty i działania wymagane do udostępnienia danych;

d) dotyczyć, w miarę możliwości, danych nieosobowych;

e) zawierać informacje dla posiadacza danych o karach nakładanych na podstawie art. 33 przez właściwy organ, o którym mowa w art. 31, w przypadku niezastosowania się do wniosku;

f) zostać podany do wiadomości publicznej w internecie bez zbędnej zwłoki.

3. Organ sektora publicznego ani instytucja, agencja lub organ Unii nie mogą danych uzyskanych na podstawie niniejszego rozdziału udostępniać do ponownego wykorzystania w rozumieniu dyrektywy (UE) 2019/1024. Dyrektywa (UE) 2019/1024 nie ma zastosowania do uzyskanych na podstawie niniejszego rozdziału danych będących w posiadaniu organów sektora publicznego.

4. Ust. 3 nie uniemożliwia organowi sektora publicznego ani instytucji, agencji lub organowi Unii wymiany danych uzyskanych na podstawie niniejszego rozdziału z innym organem sektora publicznego, instytucją, agencją lub organem Unii w celu wypełnienia zadań określonych w art. 15 ani udostępnienia danych osobie trzeciej, w przypadku gdy organ sektora publicznego lub instytucja, agencja lub organ Unii zleciły tej osobie trzeciej – w drodze publicznie dostępnej umowy – kontrole techniczne lub inne funkcje. Zastosowanie mają obowiązki spoczywające na organach sektora publicznego i instytucjach, agencjach lub organach Unii na mocy art. 19.

W przypadku gdy organ sektora publicznego lub instytucja, agencja lub organ Unii przekazują lub udostępniają dane na podstawie niniejszego ustępu, powiadamiają o tym posiadacza danych, od którego otrzymano dane.

Artykuł 18
Stosowanie się do wniosków o udostępnienie danych

1. Posiadacz danych otrzymujący wniosek o dostęp do danych na podstawie niniejszego rozdziału bez zbędnej zwłoki udostępnia dane organowi sektora publicznego lub instytucji, agencji lub organowi Unii, które wystąpiły z wnioskiem.

2. Bez uszczerbku dla określonych w przepisach sektorowych szczególnych potrzeb w zakresie dostępności danych posiadacz danych może odmówić zastosowania się do wniosku lub wystąpić o jego zmianę w ciągu 5 dni roboczych od otrzymania wniosku o udostępnienie danych niezbędnych do zareagowania na niebezpieczeństwo publiczne oraz w ciągu 15 dni roboczych w innych przypadkach

występowania wyjątkowej potrzeby, powołując się na jeden z następujących powodów:

a) dane są niedostępne;

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

3. W przypadku wniosku o udostępnienie danych niezbędnych do zareagowania na niebezpieczeństwo publiczne posiadacz danych może również odmówić zastosowania się do wniosku lub wystąpić o jego zmianę, jeżeli posiadacz danych dostarczył już żądane dane w odpowiedzi na wcześniej złożony w tym samym celu wniosek innego organu sektora publicznego lub instytucji, agencji lub organu Unii, a nie został powiadomiony o zniszczeniu danych na podstawie art. 19 ust. 1 lit. c).

4. Jeżeli posiadacz danych postanowi odmówić zastosowania się do wniosku lub wystąpić o jego zmianę zgodnie z ust. 3, musi wskazać tożsamość organu sektora publicznego lub instytucji, agencji lub organu Unii, które wcześniej złożyły wniosek w tym samym celu.

5. W przypadku gdy zastosowanie się do wniosku o udostępnienie danych organowi sektora publicznego lub instytucji, agencji lub organowi Unii wymaga ujawnienia danych osobowych, posiadacz danych czyni racjonalne kroki w celu pseudonimizacji danych, o ile wniosek można zrealizować za pomocą danych pseudonimicznych.

6. W przypadku gdy organ sektora publicznego lub instytucja, agencja lub organ Unii chce zakwestionować odmowę dostarczenia żądanych danych przez posiadacza danych lub jego wystąpienie o zmianę wniosku lub jeżeli posiadacz danych chce zakwestionować wniosek, sprawę kieruje się do właściwego organu, o którym mowa w art. 31.

Artykuł 19

Obowiązki organów sektora publicznego oraz instytucji, agencji i organów Unii

1. Organ sektora publicznego lub instytucja, agencja lub organ Unii, które otrzymały dane na podstawie wniosku złożonego na podstawie art. 14:

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

b) muszą wdrożyć – o ile konieczne jest przetwarzanie danych osobowych – środki techniczne i organizacyjne chroniące prawa i wolności osób, których dane dotyczą;

c) muszą zniszczyć dane, gdy tylko przestaną one być niezbędne do określonego celu, i poinformować posiadacza danych o ich zniszczeniu.

2. Ujawnienie tajemnicy przedsiębiorstwa lub domniemanej tajemnicy przedsiębiorstwa organowi sektora publicznego lub instytucji, agencji lub organowi Unii jest wymagane wyłącznie w zakresie, w jakim jest to absolutnie niezbędne do osiągnięcia celu wniosku. W takim przypadku organ sektora publicznego lub instytucja, agencja lub organ Unii stosują odpowiednie środki, aby zachować poufność tych tajemnic przedsiębiorstwa.

Artykuł 20
Wynagrodzenie w przypadkach wyjątkowej potrzeby

1. Dane udostępniane w celu zareagowania na niebezpieczeństwo publiczne na podstawie art. 15 lit. a) są udostępniane nieodpłatnie.

2. W przypadku gdy posiadacz danych żąda wynagrodzenia za udostępnienie danych zgodnie z wnioskiem złożonym na podstawie art. 15 lit. b) lub c), wynagrodzenie takie nie może przekraczać kosztów technicznych i organizacyjnych poniesionych w celu zastosowania się do wniosku, w tym, w stosownych przypadkach, kosztów anonimizacji i dostosowania technicznego, powiększonych o rozsądną marżę. Na żądanie organu sektora publicznego lub instytucji, agencji lub organu Unii, które wystąpiły z wnioskiem o udostępnienie danych, posiadacz danych dostarcza informacji o podstawie obliczenia kosztów i rozsądnej marży.

Artykuł 21
Wkład organizacji badawczych lub urzędów statystycznych w kontekście wyjątkowych potrzeb

1. Organ sektora publicznego lub instytucja, agencja lub organ Unii są uprawnione do udostępniania danych otrzymanych na podstawie niniejszego rozdziału osobom fizycznym lub organizacjom na potrzeby prowadzenia badań naukowych lub analiz zgodnych z celem, w którym wystąpiono o dane, lub krajowym urzędom statystycznym i Eurostatowi do celów tworzenia statystyki publicznej.

2. Osoby fizyczne lub organizacje otrzymujące dane na podstawie ust. 1 muszą prowadzić działalność o charakterze niekomercyjnym lub w kontekście misji realizowania interesu publicznego uznanej w prawie Unii lub prawie państwa członkowskiego. Nie zaliczają się do nich organizacje znajdujące się pod decydującym wpływem przedsiębiorstw komercyjnych lub takie, które z uwagi na ten wpływ mogłyby doprowadzić do udzielenia przedsiębiorstwom komercyjnym preferencyjnego dostępu do wyników badań.

3. Osoby fizyczne lub organizacje otrzymujące dane na podstawie ust. 1 muszą przestrzegać przepisów art. 17 ust. 3 i art. 19.

4. W przypadku gdy organ sektora publicznego lub instytucja, agencja lub organ Unii przekazują lub udostępniają dane na podstawie ust. 1, powiadamiają o tym posiadacza danych, od którego otrzymano dane.

Artykuł 22
Wzajemna pomoc i współpraca transgraniczna

1. Organy sektora publicznego oraz instytucje, agencje i organy Unii współpracują ze sobą i udzielają sobie wzajemnie pomocy w celu spójnego wykonywania przepisów niniejszego rozdziału.

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

3. W przypadku gdy organ sektora publicznego zamierza wystąpić z wnioskiem o udostępnienie danych do posiadacza danych mającego siedzibę w innym państwie członkowskim, najpierw powiadamia o tym zamiarze właściwy organ tego państwa członkowskiego, o którym to organie mowa w art. 31. Wymóg ten ma również zastosowanie do wniosków składanych przez instytucje, agencje i organy Unii.

4. Po otrzymaniu powiadomienia zgodnie z ust. 3 odpowiedni właściwy organ informuje organ sektora publicznego, który wystąpił z wnioskiem, o ewentualnej potrzebie współpracy z organami sektora publicznego państwa członkowskiego, w którym posiadacz danych ma siedzibę, w celu zmniejszenia obciążenia administracyjnego posiadacza danych związanego z zastosowaniem się do wniosku. Organ sektora publicznego, który wystąpił z wnioskiem, uwzględnia opinię odpowiedniego właściwego organu.

ROZDZIAŁ VI

PRZEJŚCIE NA INNE USŁUGI PRZETWARZANIA DANYCH

Artykuł 23

Usuwanie przeszkód w skutecznej zmianie dostawcy usług przetwarzania danych

1. Dostawcy usług przetwarzania danych wprowadzają środki przewidziane w art. 24, 25 i 26, aby zapewnić klientom korzystającym z ich usług możliwość przejścia na inną usługę przetwarzania danych, obejmującą ten sam rodzaj usług, świadczoną przez innego dostawcę usług. Dostawcy usług przetwarzania danych w szczególności usuwają przeszkody handlowe, techniczne, umowne i organizacyjne, które utrudniają klientom:

   a) wypowiedzenie umowy o świadczenie usługi po upływie okresu wypowiedzenia wynoszącego maksymalnie 30 dni kalendarzowych;

   b) zawarcie nowych umów z innym dostawcą usług przetwarzania danych obejmujących ten sam rodzaj usług;

   c) przenoszenie ich danych, aplikacji i innych aktywów cyfrowych do innego dostawcy usług przetwarzania danych;

   d) utrzymanie równoważności funkcjonalnej usługi w środowisku informatycznym innego dostawcy lub innych dostawców usług przetwarzania danych obejmujących ten sam rodzaj usług zgodnie z art. 26.

2. Ust. 1 ma zastosowanie wyłącznie do przeszkód związanych z usługami, umowami lub praktykami handlowymi pierwotnego dostawcy usług.

Artykuł 24

Postanowienia umowne dotyczące zmiany dostawcy usług przetwarzania danych

1. Prawa klienta i obowiązki dostawcy usług przetwarzania danych w odniesieniu do zmiany dostawcy takich usług muszą być jasno określone w pisemnej umowie. Nie naruszając przepisów dyrektywy (UE) 2019/770, ujmuje się w tej umowie co najmniej następujące elementy:

   a) klauzule umożliwiające klientowi, na jego wniosek, przejście na usługę przetwarzania danych oferowaną przez innego dostawcę usług przetwarzania danych lub przeniesienie wszystkich danych, aplikacji i aktywów cyfrowych wygenerowanych bezpośrednio lub pośrednio przez klienta do systemu lokalnego, w szczególności klauzule umożliwiające ustanowienie obowiązkowego maksymalnego okresu przejściowego wynoszącego 30 dni kalendarzowych, podczas którego dostawca usług przetwarzania danych:

1) wspomaga i – jeżeli jest to technicznie wykonalne – kończy proces zmiany dostawcy;

2) zapewnia pełną ciągłość świadczenia odpowiednich funkcji lub usług;

b) wyczerpującą specyfikację wszystkich kategorii danych i aplikacji, które można eksportować w trakcie procesu zmiany dostawcy, w tym co najmniej wszystkich danych importowanych przez klienta w momencie zawarcia umowy o świadczenie usług oraz wszystkich danych i metadanych utworzonych przez klienta i w wyniku korzystania z usługi w okresie świadczenia usługi, w tym między innymi parametrów konfiguracji, ustawień zabezpieczeń, praw dostępu i rejestrów dostępu do usługi;

c) minimalny okres, w którym można odzyskać dane, wynoszący co najmniej 30 dni kalendarzowych, rozpoczynający się po zakończeniu okresu przejściowego uzgodnionego między klientem a dostawcą usług, zgodnie z ust. 1 lit. a) i ust. 2.

2. Jeżeli obowiązkowy okres przejściowy określony w ust. 1 lit. a) i c) niniejszego artykułu jest technicznie niewykonalny, dostawca usług przetwarzania danych powiadamia o tym klienta w ciągu 7 dni roboczych od złożenia wniosku o zmianę dostawcy, należycie uzasadniając techniczną niewykonalność szczegółowym sprawozdaniem i wskazując alternatywny okres przejściowy, który nie może przekraczać 6 miesięcy. Zgodnie z ust. 1 niniejszego artykułu pełna ciągłość świadczenia usług musi być zapewniona przez cały alternatywny okres przejściowy, o którym mowa w art. 25 ust. 2.

Artykuł 25
Stopniowe wycofywanie opłat z tytułu zmiany dostawcy

1. Od dnia [data X+3 lata] r. dostawcy usług przetwarzania danych nie nakładają na klienta żadnych opłat za proces zmiany dostawcy.

2. Od dnia [data X, data wejścia w życie aktu w sprawie danych] r. do dnia [data X +3 lata] r. dostawcy usług przetwarzania danych mogą nakładać na klienta obniżone opłaty za proces zmiany dostawcy.

3. Opłaty, o których mowa w ust. 2, nie mogą przekraczać kosztów poniesionych przez dostawcę usług przetwarzania danych i bezpośrednio związanych z danym procesem zmiany dostawcy.

4. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 38 służących uzupełnieniu niniejszego rozporządzenia w celu wprowadzenia mechanizmu monitorowania umożliwiającego Komisji monitorowanie opłat za zmianę dostawcy, które nakładają na rynku dostawcy usług przetwarzania danych, w celu zapewnienia, aby wycofanie opłat z tytułu zmiany dostawcy opisane w ust. 1 niniejszego artykułu zostało osiągnięte w terminie określonym w tym samym ustępie.

Artykuł 26
Aspekty techniczne 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, przetwarzane w inny sposób lub wdrażane na tych elementach infrastruktury, muszą zapewnić klientowi po przejściu na usługę obejmującą ten sam rodzaj usługi oferowaną przez innego dostawcę usług przetwarzania danych równoważność funkcjonalną w korzystaniu z nowej usługi.

2. W przypadku usług przetwarzania danych innych niż usługi, o których mowa w ust. 1, dostawcy usług przetwarzania danych muszą udostępniać otwarte interfejsy publicznie i nieodpłatnie.

3. W przypadku usług przetwarzania danych innych niż usługi, o których mowa w ust. 1, dostawcy usług przetwarzania danych muszą zapewniać zgodność z otwartymi specyfikacjami w zakresie interoperacyjności lub normami europejskimi w zakresie interoperacyjności określonymi zgodnie z art. 29 ust. 5 niniejszego rozporządzenia.

4. Jeżeli w przypadku danego rodzaju usługi nie istnieją otwarte specyfikacje lub normy europejskie w zakresie interoperacyjności, o których mowa w ust. 3, dostawca usług przetwarzania danych na wniosek klienta eksportuje wszystkie wygenerowane lub współwygenerowane dane, w tym odpowiednie formaty danych i struktury danych, w uporządkowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

ROZDZIAŁ VII
ZABEZPIECZENIA DANYCH NIEOSOBOWYCH W KONTEKŚCIE MIĘDZYNARODOWYM

Artykuł 27
Dostęp międzynarodowy i przekazywanie międzynarodowe

1. Dostawcy usług przetwarzania danych wprowadzają wszelkie uzasadnione środki techniczne, prawne i organizacyjne, w tym ustalenia umowne, w celu zapobiegania międzynarodowemu przekazywaniu danych nieosobowych przechowywanych w Unii lub dostępowi władz do tych danych, w przypadku gdy takie przekazywanie lub dostęp są sprzeczne z prawem Unii lub prawem odpowiedniego państwa członkowskiego, nie naruszając przepisów ust. 2 ani 3.

2. Orzeczenie lub wyrok sądu lub trybunału oraz decyzja organu administracyjnego państwa trzeciego wymagające od dostawcy usług przetwarzania danych przekazania przechowywanych w Unii danych nieosobowych objętych zakresem niniejszego rozporządzenia lub udzielenia dostępu do tych danych mogą zostać uznane lub być w jakikolwiek sposób wykonalne wyłącznie wówczas, gdy opierają się na umowie międzynarodowej, takiej jak traktat o pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią lub na wszelkiej takiej umowie między wzywającym państwem trzecim a państwem członkowskim.

3. W przypadku braku takiej umowy międzynarodowej, jeżeli dostawca usług przetwarzania danych jest adresatem orzeczenia sądu lub trybunału lub decyzji organu administracyjnego państwa trzeciego wymagających przekazania przechowywanych w Unii danych nieosobowych objętych zakresem niniejszego rozporządzenia lub udzielenia dostępu do tych danych, a zastosowanie się do takiego orzeczenia lub takiej decyzji wiązałoby się z ryzykiem narażenia adresata na konflikt z prawem Unii lub z prawem krajowym danego państwa członkowskiego,

przekazanie takich danych temu organowi państwa trzeciego lub udzielenie mu dostępu do takich danych odbywa się wyłącznie w przypadku gdy:

a) system państwa trzeciego wymaga określenia powodów i proporcjonalności decyzji, orzeczenia lub wyroku oraz wymaga, aby taka decyzja, takie orzeczenie lub taki wyrok, w zależności od przypadku, miały szczególny charakter, na przykład poprzez ustanowienie wystarczającego powiązania z niektórymi osobami podejrzanymi lub naruszeniami;

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

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

Adresat decyzji może zwrócić się o opinię do odpowiednich właściwych podmiotów lub organów, zgodnie z niniejszym rozporządzeniem, w celu ustalenia, czy warunki te zostały spełnione, w szczególności jeżeli uzna, że decyzja może dotyczyć szczególnie chronionych danych handlowych lub naruszać interesy bezpieczeństwa narodowego lub obrony Unii lub jej państw członkowskich.

Europejska Rada ds. Innowacji w zakresie Danych ustanowiona rozporządzeniem [xxx – akt w sprawie zarządzania danymi] doradza Komisji i wspiera ją w opracowywaniu wytycznych dotyczących oceny spełnienia tych warunków.

4. Jeżeli spełnione są warunki określone w ust. 2 lub 3, dostawca usług przetwarzania danych dostarcza minimalną ilość danych dozwoloną w odpowiedzi na wniosek, w oparciu o jego właściwą interpretację.

5. Dostawca usług przetwarzania danych informuje posiadacza danych o istnieniu wniosku organu administracyjnego w państwie trzecim o dostęp do jego danych, zanim zastosuje się do tego wniosku, z wyjątkiem przypadków, w których wniosek służy celom egzekwowania prawa i tak długo, jak jest to konieczne do zachowania skuteczności działań w zakresie egzekwowania prawa.

ROZDZIAŁ VIII
INTEROPERACYJNOŚĆ

Artykuł 28
Zasadnicze wymagania w zakresie interoperacyjności

1. Operatorzy przestrzeni danych muszą spełniać następujące zasadnicze wymagania w celu ułatwienia interoperacyjności danych oraz mechanizmów i usług udostępniania danych:

a) zawartość zbioru danych, ograniczenia korzystania, licencje, metody gromadzenia danych, jakość danych i niepewność muszą być dostatecznie opisane, aby umożliwić odbiorcy znalezienie danych, dostęp do nich i korzystanie z nich;

b) struktury danych, formaty danych, słowniki, systemy klasyfikacji, taksonomie i wykazy kodów muszą być opisane w ogólnodostępny i spójny sposób;

c) techniczne środki dostępu do danych, takie jak interfejsy programowania aplikacji, oraz warunki korzystania z tych środków i jakość usługi muszą być dostatecznie opisane, aby umożliwić automatyczny dostęp do danych i ich przekazywanie między stronami, w tym w sposób ciągły lub w czasie rzeczywistym w formacie nadającym się do odczytu maszynowego;

d) muszą być zapewnione środki umożliwiające interoperacyjność inteligentnych umów w ramach usług i działań realizowanych przez wspomnianych operatorów.

Wymagania te mogą mieć charakter ogólny lub dotyczyć konkretnych sektorów, przy czym należy w pełni uwzględnić ich wzajemne powiązania z wymaganiami wynikającymi z innych unijnych lub krajowych przepisów sektorowych.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 38 w celu uzupełnienia niniejszego rozporządzenia poprzez sprecyzowanie zasadniczych wymagań, o których mowa w ust. 1.

3. Uznaje się, że operatorzy przestrzeni danych, którzy spełniają normy zharmonizowane lub części tych norm, do których odniesienia opublikowano w *Dzienniku Urzędowym Unii Europejskiej*, spełniają zasadnicze wymagania, o których mowa w ust. 1 niniejszego artykułu, w zakresie, w jakim wspomniane normy obejmują te wymagania.

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

5. Komisja przyjmuje – w drodze aktów wykonawczych – wspólne specyfikacje, jeżeli normy zharmonizowane, o których mowa w ust. 4 niniejszego artykułu, nie istnieją lub jeżeli uzna, że odpowiednie normy zharmonizowane są niewystarczające do zapewnienia zgodności z zasadniczymi wymaganiami określonymi w ust. 1 niniejszego artykułu, w razie potrzeby, w odniesieniu do któregokolwiek z wymagań określonych w ust. 1 niniejszego artykułu lub wszystkich tych wymagań. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

6. Komisja może przyjąć wytyczne określające specyfikacje w zakresie interoperacyjności na potrzeby funkcjonowania wspólnych europejskich przestrzeni danych, takie jak modele architektoniczne i normy techniczne wdrażające przepisy prawne i uzgodnienia między stronami sprzyjające udostępnianiu danych, na przykład dotyczące praw dostępu i technicznego tłumaczenia zgody lub pozwolenia.

Artykuł 29
Interoperacyjność usług przetwarzania danych

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

a) są ukierunkowane na osiągnięcie interoperacyjności między różnymi usługami przetwarzania danych, które obejmują ten sam rodzaj usług;

b) zwiększają możliwość przenoszenia aktywów cyfrowych między różnymi usługami przetwarzania danych, które obejmują ten sam rodzaj usług;

c) gwarantują, jeżeli jest to technicznie wykonalne, równoważność funkcjonalną różnych usług przetwarzania danych, które obejmują ten sam rodzaj usług.

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

a) aspektów interoperacyjności usług w chmurze w odniesieniu do interoperacyjności transportu, 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 muszą być zgodne z pkt 3 i 4 załącznika II do rozporządzenia (UE) nr 1025/2012.

4. Komisja może, zgodnie z art. 10 rozporządzenia (UE) nr 1025/2012, zwrócić się do co najmniej jednej europejskiej organizacji normalizacyjnej z wnioskiem o opracowanie norm europejskich mających zastosowanie do określonych rodzajów usług przetwarzania danych.

5. Do celów art. 26 ust. 3 niniejszego rozporządzenia Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 38 w celu opublikowania odniesienia do otwartych specyfikacji w zakresie interoperacyjności i norm europejskich dotyczących interoperacyjności usług przetwarzania danych w centralnym repozytorium norm Unii dotyczących interoperacyjności usług przetwarzania danych, jeżeli te specyfikacje i normy spełniają kryteria określone w ust. 1 i 2 niniejszego artykułu.

Artykuł 30

Zasadnicze wymagania dotyczące inteligentnych umów w zakresie udostępniania danych

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 umowy o udostępnienie danych, musi spełniać następujące zasadnicze wymagania:

a) odporność: zapewnienie, aby inteligentna umowa została opracowana w sposób umożliwiający bardzo wysoki poziom odporności na błędy funkcjonalne i manipulacje ze strony osób trzecich;

b) bezpieczne zakończenie i przerwanie: zapewnienie, aby istniał mechanizm umożliwiający zakończenie ciągłej realizacji transakcji: inteligentna umowa musi obejmować funkcje wewnętrzne, które mogą zresetować umowę lub polecić jej zakończenie lub przerwanie działania w celu uniknięcia przyszłego (przypadkowego) wykonywania;

c) archiwizacja i ciągłość danych: przewidzenie możliwości – w przypadku gdy inteligentna umowa musi zostać zakończona lub dezaktywowana – archiwizacji danych transakcyjnych oraz logiki i kodu inteligentnej umowy w celu zachowania rejestru operacji wykonanych na danych w przeszłości (możliwość kontroli); oraz

d) kontrola dostępu: inteligentna umowa musi być chroniona za pomocą rygorystycznych mechanizmów kontroli dostępu w warstwach zarządzania i inteligentnych umów.

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 umowy o udostępnienie danych, przeprowadza ocenę zgodności w celu spełnienia zasadniczych wymagań określonych w ust. 1 oraz 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 umowy o udostępnienie danych, są odpowiedzialni za zgodność z wymaganiami określonymi w ust. 1.

4. Uznaje się, że inteligentna umowa, która spełnia normy zharmonizowane lub odpowiednie części tych norm opracowane i opublikowane w *Dzienniku Urzędowym Unii Europejskiej,* jest zgodna z zasadniczymi wymaganiami określonymi w ust. 1 niniejszego artykułu w zakresie, w jakim wspomniane normy obejmują te wymagania.

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

6. Jeżeli normy zharmonizowane, o których mowa w ust. 4 niniejszego artykułu, nie istnieją lub jeżeli Komisja uzna, że odpowiednie normy zharmonizowane są niewystarczające do zapewnienia zgodności z zasadniczymi wymaganiami określonymi w ust. 1 niniejszego artykułu w kontekście transgranicznym, Komisja może – w drodze aktów wykonawczych – przyjąć wspólne specyfikacje w odniesieniu do zasadniczych wymagań określonych w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

ROZDZIAŁ IX
WDROŻENIE I EGZEKWOWANIE

Artykuł 31
Właściwe organy

1. Każde państwo członkowskie wyznacza właściwy organ lub właściwe organy odpowiedzialne za stosowanie i wdrażanie niniejszego rozporządzenia. Państwa członkowskie mogą ustanowić co najmniej jeden nowy organ lub oprzeć się na organach już istniejących.

2. Nie naruszając ust. 1 niniejszego artykułu:

a) niezależne organy nadzorcze odpowiedzialne za monitorowanie stosowania rozporządzenia (UE) 2016/679 są odpowiedzialne za monitorowanie stosowania niniejszego rozporządzenia w zakresie ochrony danych osobowych. Rozdziały VI i VII rozporządzenia (UE) 2016/679 stosuje się odpowiednio. Zadania i uprawnienia organów nadzorczych są wykonywane w odniesieniu do przetwarzania danych osobowych;

b) w odniesieniu do konkretnych kwestii sektorowych dotyczących wymiany danych w związku z wdrażaniem niniejszego rozporządzenia respektuje się kompetencje organów sektorowych;

c) właściwy organ krajowy odpowiedzialny za stosowanie i egzekwowanie przepisów rozdziału VI niniejszego rozporządzenia musi posiadać doświadczenie w dziedzinie usług w zakresie danych i łączności elektronicznej.

3. Państwa członkowskie zapewniają, aby odpowiednie zadania i uprawnienia właściwych organów wyznaczonych na podstawie ust. 1 niniejszego artykułu były jasno określone i obejmowały:

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

b) rozpatrywanie skarg wynikających z domniemanych naruszeń niniejszego rozporządzenia oraz prowadzenie postępowań, w odpowiednim zakresie, w przedmiocie tych skarg, a także informowanie skarżącego 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 – w drodze procedur administracyjnych – odstraszających kar pieniężnych, które mogą obejmować kary okresowe i kary z mocą wsteczną, lub wszczynanie postępowania sądowego w celu nałożenia grzywien;

e) monitorowanie postępów technologicznych mających znaczenie dla udostępniania i wykorzystywania danych;

f) współpracę z właściwymi organami innych państw członkowskich w celu zapewnienia spójnego stosowania niniejszego rozporządzenia, w tym wymianę wszystkich istotnych informacji drogą elektroniczną bez zbędnej zwłoki;

g) zapewnienie publicznej dostępności w internecie wniosków o udostępnienie danych składanych przez organy sektora publicznego w przypadku niebezpieczeństwa publicznego na podstawie przepisów rozdziału V;

h) współpracę ze wszystkimi odpowiednimi właściwymi organami w celu zapewnienia, aby obowiązki określone w rozdziale VI były egzekwowane zgodnie z innymi przepisami unijnymi i samoregulacją mającymi zastosowanie do dostawców usług przetwarzania danych;

i) zapewnienie wycofania opłat za zmianę dostawcy usług przetwarzania danych zgodnie z art. 25.

4. W przypadku gdy państwo członkowskie wyznacza więcej niż jeden właściwy organ, właściwe organy przy wykonywaniu zadań i uprawnień powierzonych im na mocy ust. 3 niniejszego artykułu współpracują ze sobą, w tym, w stosownych przypadkach, z organem nadzorczym odpowiedzialnym za monitorowanie stosowania rozporządzenia (UE) 2016/679, aby zapewnić spójne stosowanie niniejszego rozporządzenia. W takich przypadkach odpowiednie państwa członkowskie wyznaczają właściwy organ koordynujący.

5. Państwa członkowskie przekazują Komisji nazwy wyznaczonych właściwych organów oraz ich odpowiednie zadania i uprawnienia, a także, w stosownych przypadkach, nazwę właściwego organu koordynującego. Komisja prowadzi publiczny rejestr tych organów.

6. Wykonując swoje zadania i korzystając ze swoich uprawnień zgodnie z niniejszym rozporządzeniem, właściwe organy muszą pozostawać wolne od jakichkolwiek bezpośrednich i pośrednich wpływów zewnętrznych, nie mogą zwracać się do żadnego innego organu publicznego ani podmiotu prywatnego o instrukcje ani nie mogą przyjmować takich instrukcji.

7. Państwa członkowskie zapewniają, aby wyznaczone właściwe organy dysponowały niezbędnymi zasobami umożliwiającymi im odpowiednie wykonywanie swoich zadań zgodnie z niniejszym rozporządzeniem.

Artykuł 32
Prawo do wniesienia skargi do właściwego organu

1. Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej osoby fizyczne i prawne mają prawo wnieść skargę, indywidualnie lub, w stosownych przypadkach, zbiorowo, do odpowiedniego 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.

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

3. Właściwe organy współpracują w celu rozpatrywania i rozstrzygania skarg, w tym poprzez wymianę wszystkich istotnych informacji drogą elektroniczną, bez zbędnej zwłoki. Współpraca ta nie ma wpływu na specjalny mechanizm współpracy przewidziany w rozdziałach VI i VII rozporządzenia (UE) 2016/679.

Artykuł 33
Kary

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

2. Do dnia [data rozpoczęcia stosowania rozporządzenia] r. państwa członkowskie powiadamiają Komisję o tych przepisach i środkach, a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.

3. Za naruszenia obowiązków określonych w rozdziałach II, III i V niniejszego rozporządzenia organy nadzorcze, o których mowa w art. 51 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.

4. Za naruszenia obowiązków określonych w rozdziale V niniejszego rozporządzenia organ nadzorczy, o którym mowa w art. 52 rozporządzenia (UE) 2018/1725, 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 34
Modelowe postanowienia umowne

Komisja opracowuje i zaleca niewiążące modelowe postanowienia umowne dotyczące dostępu do danych i korzystania z nich, aby pomóc stronom w sporządzaniu i negocjowaniu umów przewidujących zrównoważone prawa i obowiązki wynikające z umowy.

ROZDZIAŁ X
PRAWO *SUI GENERIS* PRZEWIDZIANE W DYREKTYWIE 1996/9/WE

Artykuł 35
Bazy danych zawierające określone dane

Aby nie ograniczać wykonywania przez użytkowników prawa dostępu do takich danych i korzystania z nich zgodnie z art. 4 niniejszego rozporządzenia lub prawa do udostępniania takich danych osobom trzecim zgodnie z art. 5 niniejszego rozporządzenia, prawo *sui generis* przewidziane w art. 7 dyrektywy 96/9/WE nie ma zastosowania do baz danych zawierających dane pozyskane lub wygenerowane podczas korzystania z produktu lub powiązanej usługi.

ROZDZIAŁ XI
PRZEPISY KOŃCOWE

Artykuł 36
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) XXX [akt w sprawie danych]].”.

Artykuł 37
Zmiana w dyrektywie (UE) 2020/1828

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

„67. [Rozporządzenie Parlamentu Europejskiego i Rady (UE) XXX [akt w sprawie danych]].”.

Artykuł 38
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. 25 ust. 4, art. 28 ust. 2 i art. 29 ust. 5, powierza się Komisji na czas nieokreślony od dnia [...] r.

3. Przekazanie uprawnień, o którym mowa w art. 25 ust. 4, art. 28 ust. 2 i art. 29 ust. 5, 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. 25 ust. 4, art. 28 ust. 2 i art. 29 ust. 5 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 39
Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

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

Artykuł 40
Inne akty prawne Unii regulujące prawa i obowiązki w zakresie dostępu do danych i korzystania z nich

1. Szczegółowe obowiązki w zakresie udostępniania danych między przedsiębiorstwami, między przedsiębiorstwami a konsumentami oraz w wyjątkowych przypadkach między przedsiębiorstwami a organami publicznymi, określone w aktach prawnych Unii, które weszły w życie do dnia [xx XXX xxx] r., oraz w aktach delegowanych lub wykonawczych przyjętych na ich podstawie, pozostają bez zmian.

2. Niniejsze rozporządzenie nie narusza przepisów Unii określających, w świetle potrzeb sektora, wspólnej europejskiej przestrzeni danych lub obszaru służącego interesowi publicznemu, dalsze wymogi, w szczególności w odniesieniu do:

a) aspektów technicznych dostępu do danych;

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

c) aspektów wykraczających poza dostęp do danych i korzystanie z nich.

Artykuł 41
Ocena i przegląd

Do dnia [*dwa lata od daty rozpoczęcia stosowania niniejszego rozporządzenia*] r. 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) inne kategorie lub rodzaje danych, które mają być udostępniane;

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

c) inne sytuacje uznawane za wyjątkową potrzebę do celów art. 15;

d) zmiany w praktykach umownych dostawców usług przetwarzania danych oraz czy prowadzi to do wystarczającej zgodności z art. 24;

e) obniżenie opłat za proces zmiany dostawcy nakładanych przez dostawców usług przetwarzania danych, zgodnie ze stopniowym wycofywaniem opłat z tytułu zmiany dostawcy na podstawie art. 25.

Artykuł 42
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 [12 miesięcy od dnia wejścia życie niniejszego rozporządzenia] r.

Sporządzono w Brukseli dnia […] r.

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