P9_TA(2023)0069

Akt w sprawie danych

Poprawki przyjęte przez Parlament Europejski w dniu 14 marca 2023 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD)) ([1])

(Zwykła procedura ustawodawcza: pierwsze czytanie)

Poprawka 1

(C/2023/419)

POPRAWKI PARLAMENTU EUROPEJSKIEGO (*)

do wniosku Komisji

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 ([1]),

uwzględniając opinię Komitetu Regionów ([2]),

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 ▌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.

([1]) Sprawa została odesłana do komisji właściwej w celu przeprowadzenia negocjacji międzyinstytucjonalnych na podstawie art. 59 ust. 4 akapit czwarty Regulaminu (A9-0031/2023).
(*) Poprawki: tekst nowy lub zmieniony został zaznaczony wytłuszczonym drukiem i kursywą; symbol ▌ sygnalizuje skreślenia.
([1]) Dz.U. C 365 z 23.9.2022, s. 18.
([2]) Dz.U. C 375 z 30.9.2022, s. 112.

(2) ***W kontekście, w którym Unia Europejska jest znaczącym światowym konkurentem w przemyśle wytwórczym i liderem w dziedzinie oprogramowania przemysłowego i robotyki,*** 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, ***wartość ekonomiczną zbiorów 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.

(3) W sektorach charakteryzujących się znacznym udziałem mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw ***(MŚP)*** 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***, uniknąć rozdrobnienia rynku wewnętrznego, które mogłoby nastąpić pod wpływem krajowego prawodawstwa,*** i usunąć bariery stojące na drodze dobrze prosperującego wewnętrznego rynku danych, należy ustanowić zharmonizowane ramy określające, kto ▌jest uprawniony do ***wykorzystania dostępnych danych – zgromadzonych, uzyskanych lub w inny sposób*** generowanych przez produkty ***skomunikowane*** 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) Niniejsze rozporządzenie gwarantuje***, że producenci produktów skomunikowanych i dostawcy powiązanych usług będą projektować produkty i usługi w taki sposób, aby*** użytkownicy produktu ***skomunikowanego*** lub powiązanej usługi w Unii mogli w odpowiednim czasie uzyskać dostęp do danych ***pobranych z tego produktu lub generowanych w trakcie świadczenia*** powiązanej usługi oraz aby użytkownicy ci mogli wykorzystywać dane, w tym poprzez udostępnianie ich wybranym przez siebie osobom trzecim. Zgodnie z przepisami niniejszego rozporządzenia ***posiadacze*** danych są ▌zobowiązani do udostępnienia danych użytkownikom i ***odbiorcom danych*** 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 ▌dostęp do danych i ich wykorzystywanie na uczciwych warunkach. Niniejsze rozporządzenie nakłada również na posiadaczy danych obowiązek udostępniania ***danych*** organom sektora publicznego państw członkowskich oraz instytucjom, agencjom lub podmiotom unijnym w przypadku wystąpienia wyjątkowej potrzeby ▌. 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 ***posiadaczy*** danych do przechowywania danych, uzyskiwania do nich dostępu lub ich przetwarzania ani jako przyznających posiadaczowi danych jakiekolwiek nowe prawo do wykorzystywania danych ***pobranych z produktu skomunikowanego*** lub generowanych ***w trakcie świadczenia*** powiązanej usługi. ***W rozporządzeniu uznaje się natomiast, że użytkownicy mogą zgodzić się na udzielenie zezwoleń na dostęp do danych i wykorzystania danych pobranych z produktów skomunikowanych lub generowanych w trakcie świadczenia powiązanych usług posiadaczom danych, którzy często mogą być producentami i którzy mogą w drodze umowy z użytkownikiem świadczyć jedną powiązaną usługę lub większą liczbę powiązanych usług***.

(6) Generowanie danych ***jest funkcją projektowania przez producenta produktu skomunikowanego, w szczególności włączenia do urządzenia czujników i oprogramowania do przetwarzania danych, działań użytkownika oraz, w zależności od warunków działania, świadczenia co najmniej jednej powiązanej usługi. Wiele produktów skomunikowanych, na przykład w sektorach infrastruktury cywilnej, wytwarzania energii lub transportu, rejestruje dane dotyczące swojego środowiska lub interakcji z innymi elementami tej infrastruktury bez podejmowania jakichkolwiek działań przez użytkownika lub jakąkolwiek osobę trzecią. Takie dane mogą często mieć charakter nieosobowy i być cenne dla użytkownika lub osób trzecich, które mogą je wykorzystywać do usprawnienia swojej działalności, ogólnego funkcjonowania sieci lub systemu lub poprzez udostępnienie ich innym osobom.*** Ta sytuacja otwiera debatę dotyczącą sprawiedliwości w gospodarce cyfrowej, ponieważ dane

pobrane z produktów skomunikowanych lub generowane w trakcie świadczenia powiązanych usług stanowią istotne dane wejściowe dla usług świadczonych na rynkach niższego szczebla, usług pomocniczych oraz innego rodzaju usług. Aby zapewnić możliwość czerpania znacznych korzyści ekonomicznych ***danych*** ▌ 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. ***Ważne jest jednak również, aby kontynuować udostępnianie danych w oparciu o dobrowolne porozumienia w celu ułatwienia pobudzania opartego na danych wzrostu wartości europejskich przedsiębiorstw.***

(7) Podstawowe prawo do ochrony danych osobowych zostało zagwarantowane w szczególności w ***rozporządzeniach Parlamentu Europejskiego i Rady*** (UE) 2016/679 ([3]) i ▌(UE) 2018/1725 ([4]). W dyrektywie 2002/58/WE ***Parlamentu Europejskiego i Rady*** ([5]) 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. ***Niniejsze rozporządzenie nie powinno być rozumiane jako tworzące nową podstawę prawną dla przetwarzania danych osobowych w ramach regulowanych działań lub jako zmieniające wymogi informacyjne określone w rozporządzeniu (UE) 2016/679. W przypadku konfliktu między niniejszym rozporządzeniem a prawem Unii w dziedzinie ochrony danych osobowych lub prawem krajowym przyjętym zgodnie z takim prawem Unii, pierwszeństwo powinny mieć odpowiednie przepisy Unii lub prawo krajowe w dziedzinie ochrony danych osobowych.***

(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 ([6]), dyrektywę Parlamentu Europejskiego i Rady 2011/83/UE ([7]) oraz dyrektywę Rady 93/13/EWG ([8]), i pozostaje bez uszczerbku dla tego prawa.

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

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

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

([6]) 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).

([7]) Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady.

([8]) 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.

(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***, poza wymogami art. 3 ust. 1,*** 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 ([9]).

(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.

(13a) Niniejsze rozporządzenie ma również na celu wzmocnienie pozycji i modeli biznesowych stron trzecich, na przykład dostawców, poprzez podejście horyzontalne. Aby uwzględnić szczególną sytuację i złożoność danego sektora, po niniejszym rozporządzeniu należy przyjąć przepisy sektorowe, na przykład dotyczące przestrzeni danych dotyczących mobilności. W przepisach tych można określić dalsze uregulowania dotyczące prawa dostawców do lepszego lub bezpośredniego dostępu do danych z ich własnych inteligentnych komponentów w kwestiach takich jak monitorowanie jakości, rozwój produktów lub poprawa bezpieczeństwa, a także wyjaśnia się rolę dostawców komponentów w odniesieniu do produktów skomunikowanych.

(13b) Niniejsze rozporządzenie pozostaje bez uszczerbku dla unijnych i krajowych aktów prawnych przewidujących ochronę praw własności intelektualnej, w tym dyrektywy 2001/29/WE ([10]), dyrektywy 2004/48/WE ([11]) oraz dyrektywy (UE) 2019/790 ([12]) Parlamentu Europejskiego i Rady.

(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 ▌usługi łączności elektronicznej***, połączenia fizycznego, samego urządzenia*** (często określanych jako internet rzeczy)***,*** z ***wyjątkiem prototypów***.. Do usług łączności elektronicznej należą naziemne sieci telefoniczne, sieci telewizji kablowej, sieci satelitarne i sieci komunikacji zbliżeniowej. ***Takie produkty skomunikowane można znaleźć we wszystkich segmentach gospodarki i społeczeństwa, w tym w infrastrukturze prywatnej, cywilnej i handlowej, w pojazdach, na statkach, statkach powietrznych, w sprzętach domowych i towarach konsumpcyjnych, wyrobach medycznych i zdrowotnych lub maszynach rolniczych i przemysłowych lub też infrastrukturze wytwarzania i przesyłu energii. Dane uzyskane, wygenerowane lub zebrane przez produkt skomunikowany dostępny dla każdego posiadacza i odbiorcy danych powinny być zawsze dostępne dla właściciela produktu lub dla osoby trzeciej, na którą właściciel produktu przeniósł pewne prawa do produktu na podstawie umowy najmu lub leasingu. Do celów niniejszego rozporządzenia właściciel lub taka osoba trzecia powinni być określani jako użytkownik. Te prawa dostępu nie***

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

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

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

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

powinny w żaden sposób zmieniać praw podstawowych osób ani kolidować z prawami podstawowymi osób, których dane dotyczą i które mogą wchodzić w interakcję z produktem skomunikowanym, do danych osobowych generowanych przez produkt. Wybory projektowe producentów, wymagania użytkowników oraz, w stosownych przypadkach, przepisy sektorowe służące zaspokojeniu specyficznych dla danego sektora potrzeb i celów lub decyzje antymonopolowe powinny określać, które dane produkt skomunikowany jest w stanie udostępnić każdemu posiadaczowi danych lub odbiorcom danych w punkcie sprzedaży. Niniejsze rozporządzenie ma zastosowanie do produktów wprowadzonych do obrotu w Unii, a zatem nie ma zastosowania do produktów na etapie rozwoju, takich jak prototypy.

(15) Z kolei ***zakresem stosowania niniejszego rozporządzenia nie powinny być objęte treści lub dane uzyskane, wygenerowane lub pobrane z produktu skomunikowanego albo przekazane mu do celów przechowywania lub przetwarzania w imieniu osób trzecich, tak jak w przypadku serwerów lub infrastruktury chmury, między innymi do użytku w ramach usługi online.***

(16) Należy ***również*** określić zasady mające zastosowanie do ***powiązanych usług, które są wbudowane w produkt skomunikowany lub połączone z nim w taki sposób, że brak usługi uniemożliwiłby produktowi wykonywanie co najmniej jednej z jego funkcji, i które wiążą się z przekazywaniem danych między produktem skomunikowanym a dostawcą powiązanych usług. W przypadku gdy dostawca usługi powiązanej ma dostęp do danych z produktu skomunikowanego lub dostęp do danych wygenerowanych w trakcie świadczenia powiązanej usługi i ma prawo do wykorzystywania danych nieosobowych, zgodnie z art. 4 ust. 6, należy go uznać za posiadacza danych w odniesieniu do danych udostępnionych mu z produktu lub wygenerowanych w trakcie świadczenia powiązanej usługi. Takie powiązane usługi mogą stanowić część sprzedaży.*** Takie powiązane usługi mogą same generować dane cenne dla użytkownika niezależnie od możliwości gromadzenia danych przez produkt ***skomunikowany***, z którym są połączone. ***Takie dane mogą przedstawiać cyfryzację działań i zdarzeń z udziałem użytkownika i w związku z tym użytkownik powinien mieć do nich dostęp. Takie dane są potencjalnie cenne dla użytkownika oraz przyczyniają się do innowacji i rozwoju usług cyfrowych i innych usług chroniących środowisko, zdrowie i gospodarkę o obiegu zamkniętym, w tym szczególnie poprzez umożliwienie konserwacji i naprawy danych produktów lub rozwój produktów lub usług. Informacji uzyskanych lub wywnioskowanych z danych nieosobowych przez posiadacza danych lub odbiorcę danych po ich pobraniu z produktu skomunikowanego, innych niż informacje z danych wygenerowanych w trakcie świadczenia powiązanej usługi, nie należy uznawać za objęte zakresem niniejszego rozporządzenia.*** 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 ***świadczenie powiązanej usługi jest konieczne do utrzymania funkcjonalnego działania produktu skomunikowanego,*** dostawa usługi stanowi element umowy sprzedaży, najmu lub leasingu, niniejsze rozporządzenie powinno mieć zastosowanie. ***Ani zasilanie, ani dostarczanie łączności nie powinny być interpretowane na mocy niniejszego rozporządzenia jako powiązane usługi.***

(17) Dane ***pobrane z produktu skomunikowanego lub wygenerowane w trakcie świadczenia 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. ***dane dotyczące środowiska lub interakcji produktu skomunikowanego***, 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 ***pobrane z produktu, i być zestawiane w formacie zrozumiałym, ustrukturyzowanym, powszechnie stosowanym i nadającym się do odczytu maszynowego i obejmującym odpowiednie metadane,*** ale nie powinny być związane z danymi wynikającymi z jakiegokolwiek procesu programowego obliczającego dane pochodne tych danych, gdyż taki proces programowy może podlegać prawom własności intelektualnej. ***W przypadku gdy dane są udostępniane w formacie zaszyfrowanym, użytkownik powinien otrzymać wszelkie niezbędne środki do odszyfrowania i udostępnienia takich danych.***

(17a) Należy podejmować większe starania o skonsolidowanie gospodarki opartej na danych i zarządzania danymi. W szczególności zasadnicze znaczenie ma zwiększanie i wspieranie umiejętności korzystania z danych, tak aby użytkownicy i przedsiębiorstwa mieli świadomość i motywację, by oferować dostęp do swoich danych zgodnie z odpowiednimi przepisami, oraz by zapewniali taki dostęp. Leży to u podstaw zrównoważonego społeczeństwa opartego na danych. Rozpowszechnienie środków rozwijających umiejętności korzystania z danych oznaczałoby zmniejszenie nierówności cyfrowych i przyczyniłoby się do poprawy warunków pracy, a ostatecznie wsparłoby konsolidację i innowacyjną ścieżkę gospodarki opartej na danych w Unii. By zapewnić tworzenie wysokiej jakości miejsc pracy, trzeba zagwarantować – zwłaszcza w przypadku pracowników przedsiębiorstw typu start-up i MŚP – pozyskanie i rozwój umiejętności korzystania z danych, umożliwiające z kolei obywatelom i pracownikom zdobywanie kompetencji cyfrowych.

(18) Użytkownika produktu ***skomunikowanego*** należy rozumieć jako osobę prawną lub fizyczną, taką jak przedsiębiorstwo***, konsument lub organ sektora publicznego***, która ***nabyła produkt skomunikowany lub otrzymuje powiązane usługi, lub na rzecz której właściciel produktu skomunikowanego przekazał, na podstawie umowy najmu lub leasingu, tymczasowe prawa do korzystania z produktu skomunikowanego lub do korzystania z powiązanych usług***; Użytkownik ponosi ryzyko i czerpie korzyści z korzystania z produktu skomunikowanego, ***a zatem*** powinien być uprawniony do czerpania korzyści związanych z danymi ***pobranymi z produktu skomunikowanego*** i generowanymi przez ten produkt ***w trakcie świadczenia wszelkich powiązanych usług***.

(18a) Umiejętność korzystania z danych oznacza umiejętności, wiedzę i zrozumienie pozwalające użytkownikom, konsumentom i przedsiębiorstwom, w szczególności mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom, zyskiwać świadomość potencjalnej wartości danych, które generują, produkują i udostępniają, w kontekście ich praw i obowiązków ustanowionych w niniejszym rozporządzeniu oraz w innych rozporządzeniach unijnych w sprawie danych. Umiejętność korzystania z danych powinna wykraczać poza uczenie się o narzędziach i technologiach oraz powinna mieć na celu zdobycie przez obywateli i przedsiębiorstwa zdolności do korzystania z uczciwego rynku danych. Dlatego Komisja i państwa członkowskie powinny koniecznie, we współpracy ze wszystkimi odpowiednimi zainteresowanymi stronami, wspierać rozwój umiejętności korzystania z danych we wszystkich sektorach społeczeństwa, wśród obywateli w każdym wieku, w tym wśród kobiet i dziewcząt. W związku z tym Unia i państwa członkowskie powinny inwestować więcej w kształcenie i szkolenie, aby rozpowszechniać umiejętność korzystania z danych oraz ściśle monitorować postępy w tym obszarze. W tym duchu przedsiębiorstwa powinny również wspierać narzędzia i podejmować środki mające zapewnić umiejętność korzystania z danych wśród ich pracowników zajmujących się dostępem do danych oraz wykorzystywaniem i przekazywaniem danych, a także innych osób przetwarzających dane w ich imieniu, z uwzględnieniem ich wiedzy technicznej, doświadczenia, wykształcenia i przeszkolenia, a także użytkowników lub grupy użytkowników, których dane są tworzone lub generowane.

(19) W praktyce nie wszystkie dane generowane przez produkt ***skomunikowany*** lub powiązane usługi są łatwo dostępne dla użytkowników tego produktu lub powiązanej usługi, a możliwość przenoszenia danych generowanych przez produkty podłączone do internetu 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 ***skomunikowane*** 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 ***i aby dane te były dostępne nieodpłatnie, w kompleksowym, ustrukturyzowanym, powszechnie stosowanym i nadającym się do odczytu maszynowego formacie, w tym w celu pobierania, wykorzystywania tych danych i udostępniania ich O ile prawo Unii lub prawo państwa członkowskiego, lub odpowiednie przepisy antymonopolowe nie stanowią inaczej, takie dane powinny być dostępne na poziomie przetwarzania, w tym za pomocą oprogramowania zawartego w produkcie skomunikowanym, na które zezwala wybór projektowy producenta przed sprzedażą użytkownikowi. Dane powinny być dostępne w formacie, w jakim są otrzymywane z produktu, z minimalnymi dostosowaniami niezbędnymi, aby umożliwić ich wykorzystanie przez osobę trzecią, łącznie z powiązanymi metadanymi niezbędnymi do interpretacji i wykorzystania danych. Wymaga to usunięcia barier technicznych, aby zapewnić użytkownikom, jeżeli jest to technicznie możliwe, bezpośredni dostęp w czasie rzeczywistym do ich danych bez szeroko zakrojonych indywidualnych procedur weryfikacji. Aby ułatwić stronom trzecim dostęp do wymaganych danych, konieczny jest również racjonalny pod względem kosztów dostęp do narzędzi oprogramowania. W przypadku gdy kolejne aktualizacje lub zmiany produktu skomunikowanego przez producenta lub inną stronę prowadzą do dodatkowych dostępnych danych lub ograniczenia pierwotnie dostępnych danych, o takich zmianach należy poinformować użytkownika w kontekście aktualizacji lub zmiany. Niniejsze rozporządzenie nie nakłada obowiązku przechowywania danych dodatkowo na centralnej jednostce obliczeniowej produktu, jeżeli byłoby to nieproporcjonalne do przewidywanego wykorzystania. Nie uniemożliwia to producentowi lub posiadaczowi danych dobrowolnego uzgodnienia z użytkownikiem dokonania takiego dostosowania.***

(20) ***W przypadku współwłasności produktu skomunikowanego i świadczonych powiązanych usług,*** jeżeli kilka osób lub jednostek jest właścicielem produktu lub stroną umowy leasingu lub najmu , ***projekt*** produktu ***skomunikowanego***, powiązanej usługi lub stosowanego interfejsu ***powinien umożliwiać wszystkim osobom*** dostęp

do generowanych przez nie danych. Użytkownicy produktów ***skomunikowanych*** generujących dane zwykle muszą założyć konto użytkownika. W ten sposób ***posiadacz danych, którym może*** być producent może zidentyfikować użytkownika, a także jest to sposób komunikacji umożliwiający wykonanie i przetwarzanie wniosków o dostęp do danych. ***Do celów identyfikacji i uwierzytelniania producenci i dostawcy powiązanych usług powinni umożliwiać użytkownikom korzystanie z europejskich portfeli tożsamości cyfrowej wydanych na podstawie rozporządzenia (UE) 910/2014*** ([13]). 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. ***Konta użytkowników powinny umożliwiać im cofnięcie zgody na przetwarzanie i udostępnianie danych, a także żądanie usunięcia danych wygenerowanych w wyniku korzystania z produktu skomunikowanego, w szczególności w przypadkach gdy użytkownicy produktu zamierzają przenieść własność produktu na osobę trzecią.***

(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▌. ***Podmioty przetwarzające dane zdefiniowane w rozporządzeniu (UE) 2016/679 domyślnie nie są uznawane za posiadaczy danych, chyba że administrator danych wyznaczy im to konkretne zadanie.*** 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 ***oraz środowiska zawodowego*** i służą jako łatwy w użyciu interfejs do odtwarzania treści, pozyskiwania informacji lub uruchamiania fizycznych przedmiotów podłączonych do internetu ▌. 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 ▌, 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 ***skomunikowanym*** za pomocą wirtualnego asystenta zapewnionego przez podmiot niebędący producentem danego produktu ***skomunikowanego*** ▌.

(23) Przed zawarciem umowy dotyczącej zakupu ***produktu skomunikowanego producent lub, w stosownych przypadkach, sprzedawca powinien przekazać użytkownikowi jasne i wystarczające informacje na temat danych z produktu skomunikowanego, w tym dotyczących rodzaju, formatu, częstotliwości próbkowania i szacunkowej ilości dostępnych danych. Powinny one obejmować informacje na temat struktur danych, formatów danych, słowników, systemów klasyfikacji, taksonomii i wykazów kodów, jeżeli są dostępne, a także informacje na temat sposobu przechowywania*** danych ▌***, ich pobierania lub uzyskiwania do nich dostępu, łącznie z dostarczeniem zestawów narzędzi dla programistów czy interfejsów programowania aplikacji oraz warunkami ich wykorzystania i opisem jakości usługi***. W ramach tego obowiązku zapewnia się przejrzystość w odniesieniu do ***dostępnych*** generowanych danych oraz ułatwia się dostęp dla użytkownika. ***Obowiązek przejrzystości mógłby zostać spełniony przez posiadacza danych na przykład dzięki utrzymaniu ujednoliconego formatu adresowania zasobów (URL) w internecie, który można rozpowszechniać jako link do strony lub kod QR, odsyłający do odpowiednich informacji. Taki adres URL może zostać wskazany użytkownikowi przez producenta albo, w stosownych przypadkach, przez sprzedawcę przed zawarciem umowy zakupu produktu skomunikowanego.***

([13]) ***Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).***

W każdym wypadku konieczne jest zapewnienie użytkownikowi możliwości przechowywania informacji w sposób umożliwiający dostęp do nich w przyszłości i umożliwiający odtworzenie przechowywanych informacji w niezmienionej postaci. 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.

(23a) Powiązane usługi powinny być świadczone w taki sposób, aby dane generowane w trakcie ich świadczenia, które to dane odzwierciedlają cyfryzację działań i zdarzeń z udziałem użytkownika, były domyślnie, łatwo, bezpiecznie oraz, w stosownych przypadkach i jeżeli jest to technicznie możliwe, bezpośrednio dostępne dla użytkownika, bezpłatnie, w uporządkowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, wraz z odpowiednimi metadanymi niezbędnymi do ich interpretacji i wykorzystania. Informacji uzyskanych lub wywnioskowanych z tych danych za pomocą złożonych algorytmów własnościowych, w szczególności gdy łączą one dane wyjściowe z wielu czujników w produkcie skomunikowanym, nie powinno się uznawać za wchodzące w zakres obowiązku posiadacza danych do udostępniania danych użytkownikom lub odbiorcom danych, chyba że uzgodniono inaczej. Przed zawarciem umowy z użytkownikiem w sprawie świadczenia powiązanej usługi, która obejmuje dostęp dostawcy do danych z produktu skomunikowanego, zgodnie z art. 4 ust. 6 niniejszego rozporządzenia, dostawca powinien uzgodnić z użytkownikiem charakter, ilość, częstotliwość gromadzenia i format danych udostępnionych dostawcy powiązanych usług z produktu skomunikowanego, a także charakter i szacunkową ilość danych wygenerowanych podczas świadczenia powiązanej usługi oraz, w stosownych przypadkach, warunki dostępu użytkownika do takich danych lub ich pobierania, w tym okres, przez który dane te powinny być przechowywane.

(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 ***posiadaczy*** danych na wniosek użytkownika, który nie jest osobą, której dane dotyczą, a ponadto niniejszego rozporządzenia nie należy rozumieć jako nadającego ***posiadaczom*** danych jakiekolwiek nowe prawo do korzystania z danych ***pobranych z produktu skomunikowanego lub*** generowanych ***w trakcie świadczenia*** 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 ***zawartej w odniesieniu do danego produktu skomunikowanego***. ***W granicach rozsądku użytkownik powinien mieć możliwość odrzucenia tej umowy. Jeżeli użytkownik zdecyduje się odrzucić warunki umowne, nie powinno to uniemożliwiać mu korzystania z odnośnego produktu lub usługi, chyba że produkt lub usługa nie może funkcjonować bez akceptacji przez użytkownika warunków umownych.*** 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.

(24a) Obecnie przedsiębiorstwom często trudno jest uzasadnić koszty personelu i koszty oprogramowania, które są niezbędne do przygotowania zbiorów danych nieosobowych i produktów opartych na danych oraz oferowania ich potencjalnym kontrahentom za pośrednictwem rynków danych, w tym usług pośrednictwa w zakresie danych, zgodnie z definicją zawartą w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/868 ([14]). Istotną przeszkodą w udostępnianiu danych nieosobowych przez przedsiębiorstwa jest zatem z brak przewidywalności zwrotu inwestycji w selekcję i udostępnianie zbiorów danych i produktów zawierających dane. Aby umożliwić powstanie płynnych, skutecznych i uczciwych rynków danych nieosobowych w Unii, należy wyraźnie określić, która strona ma prawo do oferowania takich danych na rynku. Użytkownicy powinni mieć prawo do udostępniania danych nieosobowych odbiorcom danych w celach komercyjnych i niekomercyjnych. Takie

([14]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.U. L 152 z 3.6.2022, s. 1).

udostępnianie danych może być dokonywane bezpośrednio przez użytkownika, na jego wniosek przez posiadacza danych lub przez dostawców usług pośrednictwa w zakresie danych. Dostawcy usług pośrednictwa w zakresie danych, regulowani rozporządzeniem (UE) 2022/868, mogliby ułatwić stworzenie gospodarki opartej na danych poprzez nawiązanie stosunków handlowych między użytkownikami, odbiorcami danych i osobami trzecimi oraz mogą wspierać użytkowników w wykonywaniu prawa do wykorzystywania danych, na przykład poprzez zapewnienie odpowiedniej anonimizacji danych lub agregacji dostępu do danych pochodzących od wielu użytkowników indywidualnych. Aby chronić zachęty dla użytkowników do wykorzystania do celów zarobkowych danych nieosobowych pochodzących z należących do nich produktów skomunikowanych, posiadacze danych powinni mieć tylko możliwość wykorzystania do celów zarobkowych danych zagregowanych pochodzących od wielu użytkowników i nie powinni udostępniać danych nieosobowych, do których uzyskali dostęp z produktu skomunikowanego, osobom trzecim do celów handlowych lub niehandlowych innych niż wypełnienie ich zobowiązań umownych wobec użytkownika. Jednocześnie w przypadku gdy posiadacze danych uzgodnili umownie z użytkownikami prawo do korzystania z takich danych, powinni oni mieć swobodę korzystania z nich do szerokiego zakresu celów, w tym do poprawy funkcjonowania produktu skomunikowanego lub powiązanych usług, opracowania nowych produktów lub usług, wzbogacenia ich lub manipulowania nimi, lub agregowania ich z innymi danymi, w tym w celu udostępnienia powstałego zbioru danych osobom trzecim, o ile taki pochodny zbiór danych nie pozwala na identyfikację konkretnych pozycji danych udostępnionych posiadaczowi danych z produktu skomunikowanego i nie pozwala osobie trzeciej na wyprowadzenie bez znacznego wysiłku tych elementów danych ze zbioru danych.

(24b) W przypadku gdy produkty generują dane uzyskane lub wywnioskowane z innych danych generowanych przez produkt skomunikowany za pomocą złożonych algorytmów własnościowych, w tym dane stanowiące część oprogramowania zamkniętego w rozumieniu dyrektywy Parlamentu Europejskiego i Rady 2009/24/WE ([15]), dane takie należy uznać za nieobjęte zakresem niniejszego rozporządzenia i w związku z tym niepodlegające obowiązkowi udostępnienia ich użytkownikowi lub odbiorcy danych przez posiadacza danych, chyba że użytkownik i posiadacz danych uzgodnią inaczej. Dane takie powinny obejmować w szczególności informacje uzyskane za pomocą fuzji sensorycznej, wywodzenia lub wywnioskowania danych zgromadzonych w produkcie skomunikowanym z wielu czujników, przy użyciu złożonych algorytmów własnościowych. Do obowiązku udostępniania danych użytkownikom i odbiorcom danych przez posiadaczy danych należy jednak włączyć dane wywiedzione lub wywnioskowane z przetwarzania danych surowych zebranych z pojedynczego czujnika lub połączonej grupy czujników, aby umożliwić zrozumienie zgromadzonych danych w kontekście szerszych przypadków użycia poprzez określenie wielkości lub jakości fizycznej, lub zmiany wielkości fizycznej, takiej jak temperatura, ciśnienie, natężenie przepływu, pH, poziom cieczy, pozycja, przyspieszenie lub prędkość. W przepisach sektorowych należy dokładniej zdefiniować dostępne dane w oparciu o specyfikę sektora.

(24c) Co do zasady, aby sprzyjać powstawaniu płynnych, uczciwych i wydajnych rynków danych nieosobowych, użytkownicy produktów skomunikowanych powinni mieć możliwość udostępniania danych innym podmiotom, w tym do celów handlowych, przy minimalnym wysiłku prawnym i technicznym. Przed udostępnieniem danych użytkownik powinien mieć pewność, że ich udostępnienie nie pociągnie za sobą negatywnych konsekwencji prawnych. W związku z tym, w przypadku gdy pewne dane są wyłączone z obowiązku udostępniania danych użytkownikom lub odbiorcom danych przez posiadacza danych, zakres takich danych powinien zostać określony w umowie między użytkownikiem a posiadaczem danych dotyczącej świadczenia powiązanej usługi w zrozumiałym i jasnym formacie w taki sposób, aby użytkownicy mogli łatwo określić, które dane mogą udostępniać odbiorcom danych i stronom trzecim bez dalszych obowiązków w zakresie ochrony takich danych.

(24d) Istnieje wiele powodów, dla których niektóre dane generowane w trakcie korzystania z produktu pozostają niedostępne dla posiadacza danych i w związku z tym nie wchodziłyby w zakres obowiązków udostępniania danych określonych w rozdziale II. Dane mogą być bardzo zmienne (wartości rejestrowane z wysoką częstotliwością) i mogą być w ułamku sekundy lub szybko nadpisywane. Dane mogą być gromadzone wyłącznie w celu uruchomienia ściśle określonej funkcji, takiej jak działanie wycieraczek samochodowych lub reflektorów, a obecnie nie ma przypadku użycia, a projekt produktu nie przewiduje przechowywania takich danych

([15]) Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (Dz.U. L 111 z 5.5.2009, s. 16).

w produkcie ze względu na koszty związane z przechowywaniem takich danych, koszty podłączenia czujnika zbierającego dane do centralnego komponentu obliczeniowego, z którego dane mogłyby być eksportowane, oraz koszty łączności w przypadku przekazywania znacznych ilości danych. W związku z tym w przepisach sektorowych należy doprecyzować adekwatność dostępnych danych zgodnie z ich specyfiką, aby zapewnić dostępność co najmniej danych, które mają zasadnicze znaczenie dla naprawy lub serwisowania produktów skomunikowanych i powiązanych usług.

(25) W sektorach charakteryzujących się koncentracją małej liczby producentów ***lub dostawców usług powiązanych*** zaopatrujących użytkowników końcowych ***możliwość negocjowania przez użytkowników dostępu do danych przekazywanych przez produkt skomunikowany lub generowanych w trakcie świadczenia powiązanych usług jest ograniczona ze względu na siłę przetargową producenta lub dostawcy powiązanych usług.*** W takich okolicznościach ustalenia umowne mogą nie wystarczyć do osiągnięcia celu, jakim jest wzmocnienie pozycji użytkowników. Dane zwykle pozostają pod kontrolą producentów ***lub dostawców powiązanych usług***, przez co użytkownikom trudno jest korzystać z wartości danych generowanych przez sprzęt, który ***do nich należy***. 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***, rozwiązaniu kwestii bezpieczeństwa*** i osiągnięciu celów sektorowych. Ponadto ***posiadacze danych*** nie powinni wykorzystywać żadnych danych, do których ***uzyskali dostęp z produktu skomunikowanego lub wygenerowanych w trakcie świadczenia*** powiązanych ***usług***, do pozyskania informacji na temat sytuacji ekonomicznej użytkownika, jego aktywów lub metod produkcji, ani też nie powinni 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 ***produktów skomunikowanych*** lub powiązanej usługi, które generują dane, ***zastosowanie ma unijne prawo konsumenckie, dyrektywa 2005/29/WE, która ma zastosowanie do nieuczciwych praktyk handlowych, a dyrektywa*** 93/13/EWG ***ma zastosowanie do postanowień umownych,*** co ma zapewnić, aby konsument nie podlegał nieuczciwym postanowieniom umownym. W niniejszym rozporządzeniu określono, że nieuczciwe postanowienia umowne nałożone jednostronnie ▌ nie powinny być wiążące dla takiego przedsiębiorstwa.

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

(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, ***odbiorcy danych*** oferującemu 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. ***Wniosek powinien być ważny niezależnie od tego, czy został złożony przez użytkownika czy przez upoważnioną osobę trzecią działającą w imieniu użytkownika, taką jak upoważniony dostawca usług pośrednictwa w zakresie danych w rozumieniu rozporządzenia (UE) 2022/868. Posiadacze*** danych powinni zapewnić, aby dane udostępniane ***odbiorcy danych*** były tak samo dokładne, kompletne, wiarygodne i aktualne jak dane generowane w wyniku używania danego produktu ***skomunikowanego*** lub powiązanej usługi, do których to danych sam posiadacz danych może uzyskać dostęp lub jest uprawniony do uzyskania dostępu. W ramach przetwarzania danych należy ***w pełni*** 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. ***Inne zgodne z prawem cele obejmują w tym kontekście inżynierię odwrotną, jeżeli jest dozwolona zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/943 ([16]) jako zgodny z prawem środek niezależnego odkrywania know-how lub informacji, pod warunkiem że nie prowadzi do nieuczciwej konkurencji i pozostaje bez uszczerbku dla obowiązku nietworzenia konkurencyjnego produktu z wykorzystaniem danych otrzymanych na podstawie niniejszego rozporządzenia. Może to dotyczyć napraw, przedłużenia okresu eksploatacji produktu lub świadczenia usług posprzedażnych w odniesieniu do produktów skomunikowanych, jeżeli producent lub dostawca usług powiązanych zakończył produkcję lub świadczenie usług.***

(28a) ***Niniejsze rozporządzenie należy interpretować tak, że utrzymuje ono w mocy ochronę przyznaną tajemnicom przedsiębiorstwa na mocy dyrektywy (UE) 2016/943. Dlatego posiadacze danych powinni móc wymagać od użytkownika lub wybranych przez niego osób trzecich zachowania poufności danych uznawanych za tajemnicę przedsiębiorstwa. Tajemnice przedsiębiorstwa należy wskazać przed ich ujawnieniem. Posiadacze danych nie mogą jednak podważać prawa użytkowników do wnoszenia o dostęp do danych i wykorzystanie ich zgodnie z niniejszym rozporządzeniem na tej podstawie, że posiadacz danych uznaje określone dane za tajemnice przedsiębiorstwa. Posiadacz danych lub posiadacz tajemnicy przedsiębiorstwa, jeżeli nie jest nim posiadacz danych, powinien móc uzgodnić z użytkownikiem lub wybranymi przez niego osobami trzecimi odpowiednie środki służące zachowaniu poufności, w tym przez zastosowanie modelowych postanowień umownych, umów o poufności, ścisłych protokołów dostępu, standardów technicznych oraz kodeksów postępowania. Jeżeli użytkownik lub wybrane przez niego osoby trzecie nie stosują tych środków lub naruszają poufność tajemnic przedsiębiorstwa, posiadacz danych powinien móc zawiesić udostępnianie danych wskazanych jako tajemnice przedsiębiorstwa do czasu przeglądu przez koordynatora danych państwa członkowskiego. W takich przypadkach posiadacz danych powinien niezwłocznie powiadomić koordynatora danych państwa członkowskiego, w którym ma siedzibę, zgodnie z art. 31 niniejszego rozporządzenia, że zawiesił udostępnianie danych, i wskazuje, których środków nie zastosowano lub które tajemnice przedsiębiorstwa naruszono. Jeżeli użytkownik lub wybrana przez niego osoba trzecia chce zaskarżyć decyzję posiadacza danych o zawieszeniu udostępniania danych, koordynator danych powinien zdecydować w rozsądnym terminie, czy należy wznowić udostępnianie danych, a jeżeli tak, to na jakich warunkach. Komisja powinna z pomocą Europejskiej Rady ds. Innowacji w zakresie Danych opracować modelowe postanowienia umowne i powinna być w stanie opracowywać standardy techniczne. Komisja może także z pomocą Europejskiej Rady ds. Innowacji w zakresie Danych zachęcać do opracowywania kodeksów postępowania dotyczących poszanowania tajemnic przedsiębiorstwa lub praw własności intelektualnej przy przetwarzaniu danych, by wspierać osiągnięcie celu niniejszego rozporządzenia.***

(29) ***Odbiorcą danych, któremu*** dane są udostępniane, może być ***osoba fizyczna lub prawna,*** przedsiębiorstwo, organizacja badawcza lub organizacja niekomercyjna, ***lub pośrednik, w tym dostawca usług pośrednictwa w zakresie danych lub organizacje altruizmu danych zdefiniowane w rozporządzeniu (UE) 2022/868.*** Udostępniając dane ***odbiorcy danych, posiadacze*** danych nie powinni nadużywać swojej pozycji w celu uzyskania przewagi konkurencyjnej na rynkach, na których posiadacz danych i ***odbiorca danych*** mogą bezpośrednio ze sobą konkurować. ***Posiadacze danych*** nie powinni zatem wykorzystywać żadnych danych ***uzyskanych przez nich z produktu skomunikowanego lub wygenerowanych w trakcie świadczenia*** powiązanej usługi do pozyskania informacji na temat sytuacji ekonomicznej 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. ***Użytkownik powinien mieć prawo do udostępniania danych nieosobowych osobom trzecim w celach komercyjnych. Za zgodą użytkownika i z zastrzeżeniem przepisów niniejszego rozporządzenia odbiorcy danych powinni mieć możliwość przekazania osobom trzecim praw dostępu do danych udostępnionych przez użytkownika, w tym za wynagrodzeniem. Usługi pośrednictwa w zakresie danych [regulowane rozporządzeniem (UE) 2022/868] mogą wspierać użytkowników lub odbiorców danych w nawiązywaniu stosunków handlowych w dowolnym zgodnym z prawem celu na podstawie danych objętych zakresem niniejszego rozporządzenia. Mogą oni odgrywać zasadniczą rolę w agregowaniu dostępu do danych pochodzących od dużej liczby potencjalnych indywidualnych użytkowników danych, tak aby ułatwić analizę dużych zbiorów danych lub uczenie się maszyn, pod warunkiem że tacy użytkownicy zachowują pełną kontrolę nad tym, czy chcą uczestniczyć w takiej agregacji, oraz nad warunkami handlowymi, na jakich ich dane będą wykorzystywane.***

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

(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 ([17]). 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 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 ***pobierane z produktu skomunikowanego lub*** generowane ***w trakcie świadczenia*** 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 ***pobranych z produktu skomunikowanego lub*** generowanych ***w trakcie świadczenia*** powiązanej usługi oraz udostępniania takich danych ***odbiorcy danych***, 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 ***posiadacze*** danych mogą ponadto określić odpowiednie wynagrodzenie uiszczane przez ***odbiorców danych***, 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 ***posiadacze danych lub odbiorcy danych*** 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

([17]) Dz.U. L 303 z 28.11.2018, s. 59.

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, ***odbiorcy danych***, którym dane udostępniono na wniosek użytkownika, powinni przetwarzać dane wyłącznie do celów uzgodnionych z użytkownikiem i ***nie*** udostępniać ***tych danych*** innej osobie trzeciej ***bez jednoznacznego poinformowania użytkownika w odpowiednim czasie i jeżeli nie mają wyraźniej zgody użytkownika na takie udostępnienie***.

(34) ***Odbiorcy danych powinni*** jedynie uzyskać dostęp do informacji dodatkowych, które są niezbędne do świadczenia usługi zażądanej przez użytkownika. Po uzyskaniu dostępu do danych ***odbiorca danych powinien*** przetwarzać otrzymane dane wyłącznie do celów uzgodnionych z użytkownikiem bez ingerencji ze strony posiadacza danych. Odmówienie udzielenia dostępu do danych ***odbiorcy danych*** 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. ***Odbiorca danych lub posiadacz danych*** nie może ***nadmiernie utrudniać egzekwowania praw i wyborów użytkowników, w tym przez oferowanie użytkownikom wyboru w nieneutralny sposób, ani*** w żaden sposób zmuszać ***lub*** oszukiwać użytkownika ani też nim manipulować, ***lub przez*** podważanie lub ograniczanie autonomii, zdolności decyzyjnej lub wyborów użytkownika, w tym za pomocą interfejsu cyfrowego ***lub jego części, w tym jego struktury, projektu, funkcji lub sposobu obsługi***. W tym kontekście osoby trzecie ***lub posiadacze danych*** nie powinni 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 ***i posiadacze danych*** powinni wywiązywać się ze swoich obowiązków określonych w stosownych przepisach prawa Unii, ***w tym*** powinni przestrzegać wymogów określonych w dyrektywie 2005/29/WE, dyrektywie 2011/83/UE, dyrektywie 2000/31/WE i dyrektywie 98/6/WE.

(35) ***Posiadacze danych i odbiorcy danych nie powinni*** ponadto wykorzystywać danych do profilowania osób fizycznych, chyba że takie czynności przetwarzania są ściśle niezbędne do świadczenia usługi zażądanej przez użytkownika. Wymóg usunięcia danych ***osobowych***, 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 ***odbiorca danych*** jest dostawcą usługi pośrednictwa w zakresie danych w rozumieniu ***rozporządzenia (UE) 2022/868***, 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, ***MŚP*** 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 Parlamentu Europejskiego i Rady (UE) 2022/1925 ([18])*** 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 (***UE) 2022/1925*** i mając na uwadze wyjątkową zdolność tych przedsiębiorstw do pozyskiwania danych, uwzględnienie takich przedsiębiorstw

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

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 ***rozporządzenia (UE) 2022/1925***, 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) ***Z obowiązków rozdziału II powinny być wyłączone mikroprzedsiębiorstwa i małe przedsiębiorstwa.*** 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 ▌ zasady 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) ***Żadna umowa zawarta w celu udostępnienia danych nie powinna wprowadzać rozróżnienia między porównywalnymi kategoriami odbiorców danych, niezależnie od tego, czy są to duże przedsiębiorstwa czy mikroprzedsiębiorstwa, małe lub średnie przedsiębiorstwa.*** 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 ***posiadaczach*** danych. ***Komisja, angażując wszystkie zainteresowane strony, powinna opracować praktyczne wytyczne dotyczące określenia niedyskryminacyjnych warunków.*** Nie uznaje się, że stosowanie przez posiadacza danych różnych postanowień umownych dotyczących udostępniania danych ▌ 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 ***i udostępnianie*** cennych danych, w tym inwestycji w stosowne narzędzia techniczne, w niniejszym rozporządzeniu określono zasadę, zgodnie z którą ***posiadacze*** danych mogą zażądać odpowiedniego wynagrodzenia, gdy ***w stosunkach między przedsiębiorstwami*** są zobowiązani na mocy prawa do udostępnienia danych odbiorcy danych. Przepisów tych nie należy rozumieć jako przepisów określających zapłatę za same dane, ale raczej ***jako przepisy umożliwiające posiadaczom danych rozsądne wynagrodzenie za udostępnienie danych lub*** – w przypadku mikroprzedsiębiorstw, małych lub średnich przedsiębiorstw ***i organizacji badawczych korzystających z danych na zasadzie niedochodowej*** – zapłatę za poniesione ***bezpośrednie*** koszty i wymagane inwestycje związane z udostępnieniem danych. ***Komisja powinna opracować wytyczne określające szczegółowo, co uznaje się za rozsądne wynagrodzenie w gospodarce opartej na danych.***

(42a) Takie rozsądne wynagrodzenie może obejmować przede wszystkim poniesione koszty oraz, z wyjątkiem mikroprzedsiębiorstw i małych przedsiębiorstw, inwestycje potrzebne do udostępnienia danych. Te koszty mogą obejmować koszty techniczne, np. takie, które trzeba ponieść w związku ze zwielokrotnieniem danych, rozpowszechnieniem danych za pośrednictwem środków elektronicznych i przechowywaniem danych, ale nie z gromadzeniem lub tworzeniem danych. Takie koszty techniczne mogą obejmować również koszty przetwarzania niezbędne do udostępnienia danych. Koszty związane z udostępnieniem danych mogą również obejmować koszty reagowania na konkretne wniosków udostępnienia danych. Mogą być zróżnicowane w zależności od przyjętych uzgodnień dotyczących udostępnienia danych. Długoterminowe uzgodnienia między posiadaczami danych a odbiorcami danych, na przykład w formie modelu abonenckiego lub inteligentnych umów, mogłyby obniżyć koszty regularnych lub powtarzających się transakcji w relacjach biznesowych. Koszty związane z udostępnieniem danych są albo specyficzne dla danego wniosku, albo dzielone z innymi wnioskami. W tym drugim przypadku pojedynczy odbiorca danych nie powinien ponosić pełnych kosztów udostępnienia danych. Rozsądne wynagrodzenie może dodatkowo obejmować, z wyjątkiem mikroprzedsiębiorstw i małych przedsiębiorstw, marżę. Marża taka może być zróżnicowana w zależności od czynników związanych z samymi danymi, takich jak ilość, format lub charakter danych, bądź w zależności od podaży danych i popytu na nie. Może uwzględniać także koszty gromadzenia danych. Marża może zatem być mniejsza, gdy posiadacz danych zgromadził dane na potrzeby własnej działalności bez znacznych inwestycji, lub może być większa, gdy inwestycje w gromadzenie danych do celów działalności posiadacza danych są znaczne. Marża ta może również zależeć od dalszego wykorzystania danych przez odbiorcę danych. Może być ograniczona lub nawet wykluczona w sytuacjach, w których wykorzystanie danych przez odbiorcę danych nie ma wpływu na działalność posiadacza danych. Fakt, że dane są współgenerowane przez produkt skomunikowany należący do użytkownika, może również obniżyć wysokość wynagrodzenia w porównaniu z innymi sytuacjami, w których dane są generowane wyłącznie przez posiadacza danych, np. w trakcie świadczenia powiązanej usługi.

(43) W ***należycie*** 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 udostępnienie 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. ***Ten sam system powinien mieć zastosowanie do organizacji badawczych, które wykorzystują dane do celów nienastawionych na zysk.***

(45) Koszty bezpośrednie związane z udostępnieniem danych to koszty, które trzeba ponieść w związku ze zwielokrotnieniem danych, rozpowszechnieniem danych za pośrednictwem środków elektronicznych i przechowywaniem danych, ale nie z gromadzeniem lub tworzeniem danych. Koszty bezpośrednie związane z udostępnieniem danych powinny ograniczać się do odsetka kosztów, który wiąże się z danym pojedynczym wnioskiem, mając na uwadze, że niezbędne interfejsy techniczne lub powiązane oprogramowanie i łącze posiadacz danych musi zapewnić na stałe. Koszty związane z regularnym lub powtarzającym się udostępnianiem danych w ramach stosunków biznesowych można ograniczyć poprzez dokonanie długoterminowych ustaleń między posiadaczami danych i odbiorcami danych, na przykład poprzez przyjęcie modelu abonenckiego. ***Posiadacz danych, jeżeli nie jest MŚP, powinien aktywnie przedstawiać wyliczenia wykazujące, że cena jego usługi jest oparta na kosztach, wówczas, gdy wie lub powinien wiedzieć, że jego kontrahentem jest MŚP. W każdym wypadku powinien oświadczać, że jest zobowiązany do udostępniania danych MŚP po kosztach oraz do udostępnienia szczegółowych informacji na żądanie.***

(46) Nie ma potrzeby interwencji w przypadku udostępniania danych między dużymi przedsiębiorstwami lub w przypadku, gdy 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. ***W razie niewłaściwego użytku lub ujawnienia danych odbiorca danych powinien odpowiadać za szkody wyrządzone stronie, która ucierpiała na niewłaściwym użytku lub ujawnieniu tych danych, i bez zbędnej zwłoki zaspokoić żądanie posiadacza danych.***

(47) Przejrzystość jest ważną zasadą potrzebną do zadbania o to, aby wynagrodzenie żądane przez posiadacza danych było rozsądne lub – jeżeli odbiorcą danych jest ***MŚP*** – aby kwota wynagrodzenia nie przekraczała kosztów bezpośrednio związanych z udostępnieniem danych odbiorcy danych w związku z konkretnym wnioskiem. Aby ***odbiorcy danych byli*** 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 wyliczyć 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 zostanie 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. ***Organy rozstrzygania sporów powinny podawać do wiadomości publicznej roczne sprawozdania z działalności.***

(51) Jeżeli jedna ze stron ma silniejszą pozycję negocjacyjną, istnieje ryzyko, że w ramach negocjowania dostępu do danych strona ta wykorzysta swoją pozycję ze szkodą dla drugiej umawiającej się strony oraz sprawi, że dostęp do danych będzie komercyjnie mniej opłacalny, a czasem nawet niemożliwy z ekonomicznego punktu widzenia. Taki brak równowagi kontraktowej ***jest szkodliwy dla przedsiębiorstw*** nieposiadających istotnej zdolności do negocjowania warunków dostępu do danych, które to przedsiębiorstwa ze względu na brak wyboru mogą być zmuszone do zaakceptowania postanowień umownych oferowanych na zasadzie „przyjmij albo zrezygnuj". Z tego względu nieuczciwe postanowienia umowne regulujące dostęp do danych i 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 zostaną na te przedsiębiorstwa nałożone jednostronnie.

(52) W przepisach dotyczących postanowień umownych należy uwzględnić zasadę swobody zawierania umów będącą podstawową ideą, jeżeli chodzi o stosunki między przedsiębiorstwami. ▌ . Dotyczy to stosowania zasady „przyjmij albo zrezygnuj" – w takiej sytuacji ***dane*** 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 uznawać postanowienia umownego, które zostało zwyczajnie przedstawione przez jedną stronę i zaakceptowane przez ***drugie*** przedsiębiorstwo, ani też postanowienia wynegocjowanego i następnie przyjętego po zmianach przez umawiające się strony. ***Wszystkie ustalenia umowne powinny być zgodne z zasadami dotyczącymi zapewniania sprawiedliwych, rozsądnych i niedyskryminujących warunków (FRAND).***

(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 ***obowiązuje***.

(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 negocjowanie umów mogą stronom będącym podmiotami komercyjnymi ułatwić opracowane i rekomendowane przez Komisję modelowe postanowienia umowne w umowach dotyczących udostępniania danych między przedsiębiorstwami.

(56) W sytuacjach wystąpienia wyjątkowej potrzeby organy sektora publicznego lub instytucje, agencje lub organy Unii***, by podjąć*** działania w związku z niebezpieczeństwem publicznym lub w innych wyjątkowych przypadkach, mogą być zmuszone do wykorzystania danych***, które*** przedsiębiorstwo ***posiada, gromadzi w danym momencie lub które uprzednio uzyskało, zgromadziło lub wygenerowało w inny sposób i które przechowuje w momencie złożenia***

wniosku. 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 razie wystąpienia niebezpieczeństwa publicznego – takiego jak stan zagrożenia zdrowia publicznego, sytuacje wyjątkowe związane z degradacją środowiska i poważne klęski żywiołowe, w tym pogarszane skutkami zmiany klimatu, a także poważne katastrofy spowodowane przez człowieka, takie jak poważne cyberincydenty – interes publiczny wynikający z wykorzystania danych będzie nadrzędny względem interesów posiadacza danych związanych ze swobodnym dysponowaniem danymi, które posiada. W takim przypadku posiadacze danych powinni być zobowiązani do udostępnienia danych organom sektora publicznego lub instytucjom, agencjom lub organom Unii na ich wniosek***, z zastrzeżeniem warunków i innych zabezpieczeń określonych w niniejszym rozporządzeniu, w innym akcie prawnym Unii lub w prawie krajowym***. Występowanie niebezpieczeństwa publicznego ustala się na podstawie odpowiednich procedur stosowanych w państwach członkowskich lub przez odpowiednie organizacje międzynarodowe.

(58) Wyjątkowa potrzeba może ***również wynikać z sytuacji innych niż nadzwyczajne, gdy*** organ sektora publicznego jest w stanie wykazać, że dane są niezbędne do ***realizacji*** konkretnego zadania leżącego w interesie publicznym, które zostało wyraźnie wskazane ***i zdefiniowane w prawie krajowym, takiego jak zapobieżenie niebezpieczeństwu publicznemu lub pomoc w przywróceniu stanu sprzed wystąpienia niebezpieczeństwa publicznego. Z takim wnioskiem można się zwrócić tylko wtedy, gdy*** organ sektora publicznego lub instytucja, agencja lub organ Unii ***zidentyfikują konkretne dane, które są niedostępne, i tylko wtedy, gdy wyczerpią wszystkie następujące trzy alternatywne sposoby pozyskania danych: zwrócenie się z wnioskiem o dane na podstawie dobrowolnego porozumienia; zakup danych na rynku lub poleganie na istniejących obowiązkach udostępnienia danych***.

(59) Niniejsze rozporządzenie nie powinno dotyczyć, ani wykluczać, dobrowolnych ustaleń dotyczących wymiany danych ***nieosobowych*** między podmiotami prywatnymi i publicznymi. ▌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 wykroczeń administracyjnych, wykonywania sankcji karnych i kar 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 wykorzystywania 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, aby zagwarantować pewność prawa i ograniczyć do minimum obciążenia administracyjne nakładane 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 ***oparte na prawie Unii lub na prawie krajowym, konkretne,*** przejrzyste i proporcjonalne pod względem zakresu treści i poziomu szczegółowości. Należy wyraźnie i konkretnie wskazać cel wniosku i planowane wykorzystanie żądanych danych, a jednocześnie należy zadbać o odpowiednią elastyczność tak, aby podmiot występujący z wnioskiem 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. W trosce o przejrzystość ***i odpowiednie skoordynowanie*** wnioski o udostępnienie danych przedstawione przez organy sektora publicznego lub przez instytucje, agencje lub organy Unii powinny być bez zbędnej zwłoki ***przekazywane*** przez podmiot wnioskujący o udostępnienie danych ***koordynatorowi danych danego państwa członkowskiego, który zadba o ich ujęcie w*** publicznie dostępnym w internecie ***wykazie wszystkich wniosków uzasadnionych wyjątkową potrzebą***.

(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 przywróceniu stanu sprzed wystąpienia 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 ***rozporządzenia (UE) 2022/868 oraz*** dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 ([19]) 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 do celów 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 tworzenia statystyki publicznej, pod warunkiem że spełnione są warunki określone w niniejszym rozporządzeniu. ***Jeżeli zezwala na to prawo Unii lub prawo krajowe,*** organy sektora publicznego powinny również mieć możliwość udostępniania danych uzyskanych na podstawie niniejszego rozporządzenia innym organom sektora publicznego w razie wystąpienia wyjątkowych potrzeb, w związku z którymi wystosowano wniosek o udostępnienie danych***, pod warunkiem że posiadacz danych zostanie o tym na czas poinformowany, wszystkie organy będą przestrzegać takich samych przepisów dotyczących przejrzystości co pierwotny podmiot występujący z wnioskiem o udostępnienie danych oraz będą chronione tajemnice przedsiębiorstwa i inne prawa własności intelektualnej.***

(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***, lub gdy posiadacz danych nie gromadzi obecnie lub poprzednio nie zgromadził, nie otrzymał ani w inny sposób nie wygenerował żądanych danych i nie przechowuje ich w momencie złożenia wniosku***. 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 96/9/WE Parlamentu Europejskiego i Rady ([20]), posiadacze danych powinni korzystać z przysługujących im praw w sposób, który nie uniemożliwia organowi sektora publicznego i instytucjom, agencjom lub organom Unii uzyskania lub udostępnienia danych zgodnie z niniejszym rozporządzeniem.

▌

(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 ▌. 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. ***Organy sektora publicznego oraz instytucje, agencje i organy Unii powinny zadbać – w tym poprzez zastosowanie proporcjonalnych środków bezpieczeństwa, w stosownych przypadkach zgodnie z prawem Unii i prawem krajowym – o zachowanie wszelkiego rodzaju chronionego statusu danych oraz o zapobieżenie nieuprawnionemu dostępowi do nich.***

(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 ***lub posiadaczowi tajemnicy przedsiębiorstwa*** należy ***z wyprzedzeniem*** zagwarantować zachowanie poufności takich ujawnianych danych***, w tym w stosownych przypadkach poprzez zastosowanie modelowych postanowień umownych i standardów technicznych oraz kodeksów postępowania. Jeżeli organ sektora publicznego lub instytucja, agencja lub organ Unii bądź osoby trzecie, które otrzymały dane w celu wykonania zleconego im zadania, nie stosują tych środków lub naruszają poufność tajemnic przedsiębiorstwa, posiadacz danych powinien móc zawiesić udostępnianie danych wskazanych jako tajemnice przedsiębiorstwa. Decyzję o zawieszeniu udostępniania danych organ sektora publicznego lub***

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

([20]) Dyrektywa 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).

instytucja, agencja lub organ Unii bądź osoby trzecie, którym przekazano dane, mogą zakwestionować i poddać ją przeglądowi przez koordynatora danych państwa członkowskiego.

(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***, o ile wniosek jest ograniczony w czasie i zakresie oraz jest współmierny do sytuacji niebezpieczeństwa publicznego***. 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 wyjątkowej potrzeby niezwiązane z koniecznością reagowania na niebezpieczeństwo publiczne – w tym przypadki zapobiegania niebezpieczeństwu publicznemu lub przywracania stanu sprzed wystąpienia niebezpieczeństwa publicznego – w takich przypadkach posiadacze danych powinni być upoważnieni do otrzymania rozsądnego wynagrodzenia***. Niniejsze rozporządzenie nie powinno wpływać na istniejące porozumienia unijne lub krajowe przewidujące, że dane są udostępniane bezpłatnie, ani uniemożliwiać organom sektora publicznego, instytucjom, agencjom lub organom Unii oraz posiadaczom danych zawierania dobrowolnych porozumień o bezpłatnym udostępnianiu danych***.

(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***, o ile działania te są ściśle niezbędne do zareagowania na pilną potrzebę. Powinien on w odpowiednim czasie informować posiadacza danych o takim udostępnianiu danych***. 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 nienastawioną na zysk albo prowadzić działalność w kontekście misji w interesie publicznym uznanej przez państwo. Do celów niniejszego rozporządzenia za organizacje badawcze nie uznaje się organizacji znajdujących się pod decydującym wpływem przedsiębiorstw komercyjnych ***lub publicznych***, które mogą sprawować kontrolę nad daną organizacją ze względu na okoliczności strukturalne, przez co mogłoby dochodzić do udzielania preferencyjnego dostępu do wyników badań.

(69) Podstawowym warunkiem stworzenia bardziej konkurencyjnego rynku charakteryzującego się mniejszymi barierami wejścia dla nowych dostawców usług ***oraz zapewnienia większej odporności użytkowników tych usług*** jest dopilnowanie, aby klienci korzystający z usług przetwarzania danych, w tym usług w chmurze i usług przetwarzania brzegowego, mogli zmienić dostawcę usług przetwarzania danych***, bez przerw w świadczeniu usług i bez konieczności korzystania z usług kilku dostawców jednocześnie, bez nieuzasadnionych kosztów przekazywania danych. Gwarancje dotyczące skutecznej zmiany dostawcy powinny przysługiwać także klientom korzystającym z szeroko rozpowszechnionych ofert na poziomie bezpłatnym, aby uniknąć sytuacji, w której klient będzie uzależniony od jednego dostawcy. Ułatwienie podejścia wielochmurowego w przypadku klientów usług w chmurze również może przyczynić się do zwiększenia ich operacyjnej odporności cyfrowej, co zostało uznane w odniesieniu do instytucji świadczących usługi finansowe w akcie w sprawie operacyjnej odporności cyfrowej (DORA)***.

(69a) Opłaty z tytułu zmiany dostawcy to opłaty nakładane na klientów przez dostawców usług przetwarzania w chmurze za proces zmiany dostawcy. Zwykle opłaty te mają na celu przeniesienie kosztów, które wyjściowy dostawca może ponieść w związku z procesem zmiany, na klienta, który chce zmienić dostawcę. Przykładami powszechnych opłat z tytułu zmiany dostawcy są koszty związane z przekazaniem danych od jednego dostawcy do drugiego lub do systemu lokalnego („opłata za odejście") lub koszty konkretnych działań wspierających podczas procesu zmiany. Nieuzasadnione wysokie opłaty za odejście i inne nieuzasadnione opłaty niezwiązane z rzeczywistymi kosztami zmiany dostawcy utrudniają klientom tę zmianę, ograniczają swobodny przepływ danych, mogą ograniczać konkurencję i powodować efekt uzależnienia klientów usług przetwarzania danych od jednego dostawcy, gdyż zmniejszają motywację do wyboru innego lub dodatkowego dostawcy usług. Z racji nowych obowiązków przewidzianych niniejszym rozporządzeniem wyjściowy dostawca usług przetwarzania danych może zlecać niektóre zadania na zasadzie outsourcingu i wypłacać podmiotom trzecim wynagrodzenie w celu wypełnienia tych obowiązków. Klient nie powinien ponosić kosztów wynikających z outsourcingu poniesionych przez dostawcę usług przetwarzania danych w trakcie procesu zmiany dostawcy, a zatem takie koszty należy uznać za nieuzasadnione. Przepisy aktu w sprawie danych nie uniemożliwiają klientowi wynagradzania podmiotów trzecich za wsparcie w procesie migracji. Opłaty za odejście są nakładane na klientów przez dostawców wyjściowych usług przetwarzania danych, w przypadku gdy klienci chcą przenieść swoje dane

z sieci dostawcy usług w chmurze do lokalizacji zewnętrznej, w szczególności w przypadku zmiany jednego dostawcy na co najmniej jednego dostawcę docelowego, lub gdy chcą przenieść dane z jednej lokalizacji do innej, korzystając z usług tego samego dostawcy usług w chmurze. W związku z tym, aby zwiększyć konkurencję, stopniowe wycofywanie opłat związanych ze zmianą dostawcy usług przetwarzania danych obejmuje w szczególności zniesienie opłat za odejście pobieranych od klienta przez dostawcę usług przetwarzania danych.

(70) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 wspiera dostawców usług ***przetwarzania danych*** w skutecznym opracowywaniu i wdrażaniu samoregulacyjnych kodeksów postępowania obejmujących między innymi najlepsze praktyki w zakresie ułatwiania zmiany dostawców usług ***przetwarzania danych*** i przenoszenia danych. Mając na uwadze ***ograniczone korzystanie z*** samoregulacyjnych ram opracowanych w związku z tym rozporządzeniem oraz ogólną niedostępność otwartych standardów i interfejsów, konieczne jest przyjęcie zestawu minimalnych obowiązków regulacyjnych, które będą spoczywać na dostawcach usług przetwarzania danych, w celu wyeliminowania umownych, ***handlowych, organizacyjnych,*** ekonomicznych i technicznych przeszkód***, w tym zmniejszenia szybkości transferu danych przy odejściu klienta, utrudniającego*** skuteczną zmianę dostawcy usług przetwarzania danych.

(71) Usługi przetwarzania danych powinny obejmować usługi umożliwiające ***wszechobecny sieciowy*** dostęp na żądanie do ***konfigurowalnego***, skalowalnego i elastycznego ***wspólnego zbioru*** rozproszonych zasobów obliczeniowych. Te zasoby obliczeniowe obejmują takie zasoby jak sieci, serwery lub inną wirtualną lub fizyczną infrastrukturę, oprogramowanie, w tym narzędzia do tworzenia oprogramowania, pamięć, aplikacje i usługi. ***Modele rozmieszczenia usług przetwarzania danych powinny obejmować chmurę prywatną i publiczną. Takie usługi i modele ich rozmieszczenia powinny być takie same jak określone w normach międzynarodowych.*** Zdolność klienta korzystającego z usługi przetwarzania danych do jednostronnego zapewnienia sobie możliwości obliczeniowych, takich jak czas serwera lub pamięć sieciowa, bez żadnej ingerencji człowieka ze strony dostawcy ***usług przetwarzania danych***, można określić jako ***wymagającą minimalnego wysiłku pod względem zarządzania i związaną z minimalną interakcją między dostawcą a klientem***. Pojęcia „***wszechobecne***" używa się do opisu sytuacji, 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 ***usług*** przetwarzania danych niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania. Pojęcia „elastyczne" używa się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie od zapotrzebowania, aby szybko zwiększać lub zmniejszać dostępne zasoby w zależności od obciążenia. Pojęcia „***wspólny zbiór***" używa się do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy współdzielą 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 od 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. ***Usług cyfrowych uznawanych za platformę internetową w rozumieniu art. 3 lit. i) [aktu o usługach cyfrowych] ani usługi online w zakresie treści zdefiniowanej w art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/1128 ([21]) nie należy uznawać za „usługi przetwarzania danych" w rozumieniu niniejszego rozporządzenia.***

(71a) Usługi przetwarzania danych należą do co najmniej jednego z następujących trzech modeli świadczenia usług przetwarzania danych: IaaS (infrastruktura jako usługa), PaaS (platforma jako usługa) i SaaS (oprogramowanie jako usługa). Te modele świadczenia usług stanowią konkretne gotowe pakiety zasobów informatycznych oferowane przez dostawcę usług przetwarzania danych. Trzy podstawowe modele świadczenia usług w chmurze są

([21]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1128 z dnia 14 czerwca 2017 r. w sprawie transgranicznego przenoszenia na rynku wewnętrznym usług online w zakresie treści (Dz.U. L 168 z 30.6.2017, s. 1).

dodatkowo uzupełnione nowymi opcjami, z których każda jest innym pakietem zasobów informatycznych, takimi jak StaaS (przechowywanie jako usługa) i DBaaS (baza danych jako usługa). Do celów niniejszego rozporządzenia usługi przetwarzania danych można umieścić w bardziej szczegółowym i niewyczerpującym zbiorze przeróżnych „równoważnych usług", czyli zestawów usług przetwarzania danych, które mają ten sam główny cel i te same główne funkcje, a także opierają się na tym samym rodzaju modeli przetwarzania danych, niezwiązanych z charakterystyką operacyjną usługi. Na przykład dwie bazy danych mogą pozornie mieć ten sam podstawowy cel, ale po analizie ich modelu przetwarzania danych, modelu dystrybucji i ukierunkowanego przypadku użycia takie bazy danych należy zaliczyć do bardziej szczegółowej podkategorii równoważnych usług. Równoważne usługi mogą mieć odmienne i konkurencyjne cechy, takie jak wydajność, bezpieczeństwo, odporność i jakość usług.

(71b) ***Ekstrakcja należących do klienta danych od dostawcy wyjściowych usług przetwarzania pozostaje jednym z wyzwań, które utrudniają przywrócenie funkcji usług w infrastrukturze dostawcy usług docelowych. Z myślą o właściwym zaplanowaniu strategii odejścia, uniknięciu zbędnych i uciążliwych zadań oraz o zagwarantowaniu, że klient nie straci żadnych danych w wyniku procesu zmiany dostawcy, dostawca wyjściowych usług przetwarzania danych powinien ująć w umowie obowiązkowe informacje na temat zakresu danych, które klient może eksportować po podjęciu decyzji o zmianie dostawcy usług przetwarzania danych lub o przejściu na lokalną infrastrukturę ICT. Zakres danych eksportowalnych powinien obejmować co najmniej dane wejściowe i wyjściowe, w tym odpowiednie formaty danych, struktury danych i metadane generowane bezpośrednio lub pośrednio lub współgenerowane przez klienta w wyniku korzystania z usługi przetwarzania danych, które można wyraźnie przypisać temu klientowi. Z danych eksportowalnych należy wyłączyć wszelkie usługi przetwarzania danych, aktywa osoby trzeciej lub dane chronione prawami własności intelektualnej lub stanowiące tajemnicę przedsiębiorstwa bądź informacje poufne, takie jak dane związane z integralnością i bezpieczeństwem usługi świadczonej w ramach usługi przetwarzania danych, a także dane wykorzystywane przez dostawcę do obsługi, utrzymywania i udoskonalania usługi.***

(72) Niniejsze rozporządzenie ma ułatwić zmianę dostawcy usług przetwarzania danych, przy czym takie przejście obejmuje wszystkie ***odnośne*** 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 dalszego korzystania z danych usług w nowym środowisku ▌ z zachowaniem równoważności funkcjonalnej. ***Należy zaznaczyć, że usługi przetwarzania danych to usługi, w przypadku których przetwarzanie danych, zgodnie z definicją zawartą w niniejszym rozporządzeniu, stanowi element podstawowej działalności dostawcy usług.*** 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 kontenery. ***Zmiana dostawcy to operacja podejmowana z inicjatywy klienta i obejmująca trzy główne etapy, a mianowicie (i) ekstrakcję danych, tj. pobranie danych z ekosystemu dostawcy wyjściowego; (ii) transformację, podczas której dane są strukturyzowane w sposób, który nie odpowiada schematowi lokalizacji docelowej; i (iii) załadowanie danych do nowej lokalizacji docelowej. W szczególnej sytuacji opisanej w niniejszym rozporządzeniu za zmianę należy uznać również wyłączenie danej usługi z umowy i przeniesienie jej do innego usługodawcy. Procesem zmiany dostawcy zarządza niekiedy w imieniu klienta podmiot będący osobą trzecią. W związku z tym wszystkie prawa i obowiązki klienta ustanowione niniejszym rozporządzeniem, w tym obowiązek współpracy w dobrej wierze, należy rozumieć jako mające zastosowanie do takiego podmiotu będącego osobą trzecią w takich okolicznościach. Dostawcy usług w chmurze i ich klienci ponoszą odpowiedzialność na różnych poziomach, w zależności od etapu tego procesu. Na przykład dostawca wyjściowych usług przetwarzania danych jest odpowiedzialny za ekstrakcję danych do formatu nadającego się do odczytu maszynowego, ale to klient i dostawca usług docelowych załadują dane do nowego środowiska, chyba że została zamówiona konkretna profesjonalna usługa przeniesienia danych. W procesie zmiany dostawcy występują przeszkody o różnym charakterze, zależnie od etapu tego procesu.*** „Równoważność funkcjonalna" oznacza ***możliwość przywrócenia na podstawie danych klienta*** minimalnego poziomu funkcjonalności danej usługi ***w środowisku nowej usługi przetwarzania danych*** po zmianie dostawcy***, przy czym docelowa usługa dostarcza porównywalny rezultat w reakcji na te same dane wejściowe jak w przypadku wspólnych funkcji dostarczanych klientowi na podstawie umowy. Różne*** usługi ***mogą osiągnąć równoważność funkcjonalną w odniesieniu do wspólnych funkcji podstawowych tylko wtedy, gdy zarówno dostawcy usług wyjściowych, jak i dostawcy usług docelowych oferują niezależnie od siebie te same funkcje podstawowe. Niniejsze rozporządzenie nie ustanawia obowiązku ułatwiania równoważności funkcjonalnej modeli świadczenia usług przetwarzania danych PaaS lub SaaS.*** Zgodnie z przepisami niniejszego rozporządzenia dotyczącymi zmiany dostawcy można również przenieść ***odnośne*** metadane wygenerowane w wyniku korzystania z usługi przez klienta***, które wchodzą w zakres definicji danych eksportowalnych. Usługi***

przetwarzania danych są wykorzystywane w różnych sektorach i różnią się pod względem złożoności i rodzaju. Jest to istotna kwestia z punktu widzenia procesu przenoszenia i ram czasowych.

(72a) Potrzebne jest ambitne i zachęcające do innowacji podejście regulacyjne do interoperacyjności, aby przezwyciężyć uzależnienie od jednego dostawcy, które osłabia konkurencję i rozwój nowych usług. Interoperacyjność między równoważnymi usługami przetwarzania danych obejmuje wiele interfejsów i warstw infrastruktury i oprogramowania i rzadko ogranicza się do testu, czy jest osiągalna, czy nie. Wręcz przeciwnie, uzyskanie takiej interoperacyjności podlega analizie kosztów i korzyści, która jest niezbędna do ustalenia, czy warto dążyć do racjonalnie przewidywalnych wyników. Norma ISO/IEC 19941:2017 jest ważnym punktem odniesienia w kontekście osiągnięcia celów niniejszego rozporządzenia, ponieważ obejmuje aspekty techniczne wyjaśniające złożoność takiego procesu.

(73) Jeżeli dostawcy usług przetwarzania danych są z kolei klientami korzystającymi z usług przetwarzania danych świadczonych przez dostawcę zewnętrznego, sami będą korzystać ze skuteczniejszej możliwości zmiany dostawcy, 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 ***unikania i do eliminowania wszystkich odnośnych przeszkód oraz do*** oferowania ***w ramach swoich zdolności i proporcjonalnie do swoich obowiązków*** wszelkiej pomocy i wsparcia, które są potrzebne, aby proces zmiany dostawcy odbył się pomyślnie oraz był ***bezpieczny*** i skuteczny***. Niniejsze rozporządzenie nie zobowiązuje dostawców*** usług przetwarzania danych ***do stworzenia*** nowych kategorii usług ***przetwarzania danych***, ***w tym*** 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. ***Dostawca wyjściowych usług przetwarzania danych nie ma dostępu ani wglądu w środowisko dostawcy docelowych usług przetwarzania danych i nie powinien być zobowiązany do odtworzenia usług klienta zgodnie z wymogami równoważności funkcjonalnej w ramach infrastruktury dostawcy docelowego. Dostawca wyjściowych usług przetwarzania danych podejmuje natomiast w granicach swoich uprawnień wszelkie rozsądne działania, aby ułatwić osiągnięcie równoważności funkcjonalnej, zapewniając zasoby, odpowiednie informacje, dokumentację, wsparcie techniczne oraz, w stosownych przypadkach, niezbędne narzędzia. Informacje udzielane przez dostawcę usług przetwarzania danych klientowi powinny pomóc w opracowaniu strategii odejścia klienta i obejmować procedury inicjowania zmiany dostawcy usługi w chmurze, formaty danych nadające się do odczytu maszynowego, do których dane użytkownika mogą być wyeksportowane, narzędzia, w tym co najmniej jeden otwarty interfejs przenoszenia danych przewidziany do celów eksportu danych, informacje o znanych ograniczeniach technicznych i innych ograniczeniach, które mogą mieć wpływ na proces zmiany dostawcy, a także szacowany czas niezbędny do zakończenia*** procesu zmiany dostawcy. ***Pisemna umowa określająca prawa klienta i obowiązki dostawcy usług w chmurze powinna zawierać wyłącznie informacje dostępne dostawcy usług przetwarzania danych w momencie zawierania umowy***. Niniejsze rozporządzenie nie powinno mieć wpływu na istniejące prawa związane z rozwiązywaniem umów, w tym prawa wprowadzone rozporządzeniem (UE) 2016/679 i dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/770 ([22]). ***Obowiązkowy okres ustanowiony na mocy niniejszego rozporządzenia nie powinien naruszać innych terminów określonych w przepisach sektorowych. Rozdział VI niniejszego rozporządzenia nie powinien stać na przeszkodzie temu, by dostawca usług przetwarzania danych gwarantował swoim klientom nowe i udoskonalone usługi, cechy czy funkcje, ani temu, by konkurował na tej podstawie z innymi dostawcami usług przetwarzania danych.***

(75) Aby ułatwić zmianę dostawcy 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 bardziej wyważonych stosunków między użytkownikami a dostawcami usług ***przetwarzania danych*** oraz większej pewności prawa w kwestii warunków mających zastosowanie do zmiany dostawcy usług przetwarzania danych. W związku z tym użytkownicy i dostawcy usług ***przetwarzania danych*** powinni rozważyć posługiwanie się standardowymi klauzulami umownymi opracowanymi przez odpowiednie organy lub grupy ekspertów ustanowione na mocy prawa Unii.

([22]) 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).

(75a) ***Aby ułatwić zmianę dostawcy usług przetwarzania w chmurze, wszystkie zaangażowane strony, w tym dostawcy usług przetwarzania danych wyjściowych i docelowych, powinny współpracować w dobrej wierze, tak aby umożliwić pomyślny proces zmiany dostawcy oraz bezpieczne i terminowe przekazanie niezbędnych danych w powszechnie używanym formacie nadającym się do odczytu maszynowego oraz za pomocą otwartego standardowego interfejsu przenoszenia danych, a także aby uniknąć zakłóceń w świadczeniu usług.***

(75b) ***Usługi przetwarzania danych, które dotyczą usług w istotny sposób zmienionych tak, aby dostosować je do konkretnych potrzeb klienta (usługi na zamówienie) lub usługi przetwarzania danych świadczone na okres próbny lub służące jedynie do testowania i oceny w odniesieniu do ofert produktów biznesowych, powinny być zwolnione z niektórych obowiązków mających zastosowanie do zmiany dostawcy usług przetwarzania danych.***

(75c) ***Niezależnie od prawa do wszczęcia postępowania przed sądem, klienci powinni mieć dostęp do certyfikowanych organów rozstrzygania sporów, które rozstrzygają spory związane ze zmianą dostawcy usług przetwarzania danych.***

(76) Otwarte specyfikacje i normy w zakresie interoperacyjności ***i przenoszenia*** opracowane zgodnie z pkt 3 i 4 załącznika II do rozporządzenia ***Parlamentu Europejskiego i Rady*** (UE) 1025/2012 ***([23])*** w obszarze interoperacyjności i przenoszenia umożliwiają tworzenie ▌środowiska chmury obliczeniowej bazującego na usługach świadczonych przez wielu dostawców, co stanowi kluczowy wymóg w kontekście otwartych innowacji w europejskiej gospodarce opartej na danych. Ponieważ nie zostało dowiedzione, że procesy rynkowe mogą skutkować ustanowieniem specyfikacji i norm technicznych umożliwiających zapewnienie skutecznej interoperacyjności ***i przenoszenia*** usług w chmurze na poziomie PaaS ▌ i SaaS ▌, Komisja – na podstawie niniejszego rozporządzenia i zgodnie z rozporządzeniem (UE) nr 1025/2012 – powinna móc – ***jeżeli jest to technicznie wykonalne*** – wystąpić do europejskich organizacji normalizacyjnych z wnioskiem o opracowanie takich norm ***dla równoważnych usług***, jeżeli takie normy jeszcze nie istnieją. Ponadto Komisja będzie zachęcać podmioty obecne na rynku do opracowania odpowiednich otwartych specyfikacji w zakresie interoperacyjności ***i przenoszenia***. ***Po konsultacji z zainteresowanymi stronami i po uwzględnieniu odpowiednich międzynarodowych i europejskich norm i inicjatyw samoregulacyjnych*** Komisja może – w drodze aktów delegowanych – nakazać stosowanie europejskich norm w zakresie interoperacyjności ***i przenoszenia*** lub otwartych specyfikacji w zakresie interoperacyjności ***i przenoszenia*** do określonych ***równoważnych usług*** poprzez odniesienie w centralnym repozytorium norm Unii do interoperacyjności usług przetwarzania danych. ***Dostawcy usług przetwarzania danych powinni gwarantować zgodność z tymi normami i specyfikacjami w zakresie interoperacyjności i przenoszenia, biorąc pod uwagę charakter, bezpieczeństwo i integralność danych, które przechowują.*** Normy europejskie ***dotyczące interoperacyjności i przenoszenia usług przetwarzania danych*** oraz 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 1025/2012 i jak 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 lub udzielanie dostępu administracji rządowej do takich danych znajdujących się poza ich granicami, w tym w Unii. Wyroki sądów lub trybunałów czy decyzje innych organów sądowych lub administracyjnych, w tym organów ścigania w państwach trzecich, nakazujące przekazanie danych nieosobowych lub udzielenie dostępu do nich powinny być wykonalne, jeżeli mają za podstawę umowę międzynarodową – np. traktat o pomocy prawnej – obowiązującą między występującym państwem trzecim a Unią lub państwem członkowskim. W innych przypadkach może się zdarzyć, że wniosek o przekazanie danych nieosobowych lub udzielenie dostępu do nich wynikający z prawa państwa trzeciego pozostaje w sprzeczności z obowiązkiem ochrony takich 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

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

ochroną tajemnic przedsiębiorstwa, oraz ochroną praw własności intelektualnej, w tym z zobowiązaniami umownymi dotyczącymi poufności zgodnie z tym prawem. W przypadku braku umów międzynarodowych regulujących takie kwestie przekazanie lub dostęp powinny być dozwolone tylko wtedy, gdy zostanie sprawdzone, że system prawny państwa trzeciego wymaga określenia powodów i proporcjonalności decyzji, że wyrok sądu lub decyzja mają charakter szczegółowy oraz że uzasadniony sprzeciw adresata podlega kontroli właściwego sądu w państwie trzecim, który jest uprawniony do należytego uwzględnienia odpowiednich interesów prawnych dostawcy takich danych. Zawsze, gdy to możliwe na mocy warunków wniosku o udostępnienie danych złożonego przez organ państwa trzeciego, dostawca usług przetwarzania danych powinien mieć możliwość poinformowania ***konsumenta***, 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 chroniące obywateli Unii, sektor publiczny i przedsiębiorstwa i 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 niniejszemu aktowi, 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 ***umożliwiających*** interoperacyjność ***i przenoszenie*** powinny odgrywać normalizacja i interoperacyjność semantyczna ***i syntaktyczna***. W celu ułatwienia zgodności z wymogami dotyczącymi interoperacyjności ***we wspólnych europejskich przestrzeniach danych, które są specyficzne dla danego celu lub sektora bądź międzysektorowe, należy opracować interoperacyjne ramy wspólnych norm i praktyk do celów wymiany lub wspólnego przetwarzania danych na potrzeby m.in. opracowywania nowych produktów i usług, badań naukowych lub inicjatyw społeczeństwa obywatelskiego. Niniejsze rozporządzenie ustanawia pewne zasadnicze wymogi dotyczące interoperacyjności. Wymogi te powinni spełniać uczestnicy przestrzeni danych, którzy są podmiotami ułatwiającymi udostępnianie danych lub zaangażowanymi w nie we wspólnych europejskich przestrzeniach danych. Zgodność z tymi zasadami można uzyskać dzięki przestrzeganiu wymogów ustanowionych niniejszym rozporządzeniem lub dzięki dostosowaniu się do już istniejących norm poprzez domniemanie zgodności. W celu ułatwienia zgodności z wymogami dotyczącymi interoperacyjności*** należy przewidzieć domniemanie zgodności rozwiązań interoperacyjnych spełniających normy zharmonizowane lub ich części zgodnie z rozporządzeniem ▌ (UE) nr 1025/2012. ***Normy należy opracowywać w sposób otwarty, neutralny technologicznie i inkluzywny, zgodnie z rozdziałem II rozporządzenia (UE) nr 1025/2012. Przy uwzględnieniu, w stosownych przypadkach, stanowisk Europejskiej Rady ds. Innowacji w zakresie Danych przyjętych zgodnie z art. 30 lit. f) rozporządzenia (UE) 2022/868*** Komisja powinna przyjąć wspólne specyfikacje w obszarach, w których nie istnieją normy zharmonizowane lub w których są one niewystarczające, aby jeszcze bardziej zwiększyć interoperacyjność wspólnych europejskich przestrzeni danych, interfejsów programowania aplikacji, zmiany dostawcy usług w chmurze oraz inteligentnych umów. Ponadto w poszczególnych sektorach nadal można byłoby przyjmować wspólne specyfikacje zgodnie z unijnym lub krajowym prawem sektorowym, z uwzględnieniem szczególnych potrzeb tych sektorów. Część specyfikacji technicznych w zakresie interoperacyjności semantycznej ***mogłyby*** również stanowić struktury i modele danych wielokrotnego użytku (w formie słowników podstawowych), ontologie, profile aplikacji metadanych, dane referencyjne w formie słowników podstawowych, taksonomie, wykazy kodów, tabele uprawnień oraz tezaurusy. Ponadto***, po przeprowadzeniu konsultacji z zainteresowanymi stronami oraz po uwzględnieniu odpowiednich międzynarodowych i europejskich norm i inicjatyw samoregulacyjnych, a w stosownych przypadkach stanowisk przyjętych przez Europejską Radę ds. Innowacji w zakresie Danych, o których mowa w art. 30 lit. f) rozporządzenia (UE) 2022/868,*** Komisja powinna mieć możliwość ***przyjęcia wspólnych specyfikacji w obszarach, w których nie istnieją normy zharmonizowane, oraz możliwość*** zlecenia opracowania norm zharmonizowanych w zakresie interoperacyjności ***i przenoszenia*** usług przetwarzania danych. ***Europejska Rada ds. Innowacji w zakresie Danych powinna wzorować się na istniejących europejskich i światowych inicjatywach na rzecz międzysektorowej interoperacyjności danych. W szczególności Europejska Rada ds. Innowacji w zakresie Danych powinna w tym celu zbadać potencjał ram cyfrowej tożsamości przedmiotów, ustanowionych rozporządzeniem (UE) nr 910/2014, oraz systemów identyfikacji podmiotów prawnych, takich jak GLEIF.***

(79a) W trosce o jeszcze bardziej skoordynowane egzekwowanie niniejszego rozporządzenia Europejska Rada ds. Innowacji w zakresie Danych powinna wspierać wzajemną wymianę informacji między właściwymi organami, a także doradzać Komisji i wspierać ją w kwestiach objętych zakresem niniejszego rozporządzenia, które wchodzą w zakres kompetencji Rady określonych w art. 30 rozporządzenia (UE) 2022/868. W konsultacjach powinna stale uczestniczyć podgrupa ds. zaangażowania zainteresowanych stron, o której mowa w art. 29 ust. 2 lit. c) tego rozporządzenia.

(80) Aby promować interoperacyjność inteligentnych umów w aplikacjach do udostępniania danych, ***konieczne może być określenie*** zasadniczych wymogów dotyczących inteligentnych umów dla specjalistów, którzy tworzą inteligentne umowy dla innych osób lub włączają takie inteligentne umowy do aplikacji wspierających realizację umów o udostępnianie danych. ***Na przykład*** inteligentne umowy ***powinny gwarantować przestrzeganie warunków udostępniania danych. Należy propagować specjalne programy szkoleniowe dotyczące*** inteligentnych umów ***wśród przedsiębiorstw, a zwłaszcza MŚP***.

(81) Aby zapewnić skuteczne wdrożenie niniejszego rozporządzenia, państwa członkowskie powinny wyznaczyć co najmniej jeden właściwy organ ***i przydzielić mu wystarczające zasoby***. Jeżeli państwo członkowskie wyznaczy więcej niż jeden właściwy organ, powinno również wyznaczyć właściwy organ koordynujący. ***Aby zapewnić skuteczne wdrożenie i egzekwowanie niniejszego rozporządzenia,*** właściwe organy powinny ze sobą współpracować ***skutecznie i terminowo oraz zgodnie z zasadami dobrej administracji i wzajemnej pomocy***. 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. ***Właściwe organy powinny współpracować na wniosek organów w ramach Europejskiej Rady Ochrony Danych i Europejskiej Rady ds. Innowacji w Zakresie Danych.***

(81a) W trosce o jeszcze bardziej skoordynowane egzekwowanie niniejszego rozporządzenia Europejska Rada ds. Innowacji w Zakresie Danych powinna wspierać wzajemną wymianę informacji między właściwymi organami, a także doradzać Komisji i wspierać ją w kwestiach objętych zakresem niniejszego rozporządzenia, ze szczególnym uwzględnieniem kwestii wchodzących w zakres kompetencji Rady zgodnie z art. 30 rozporządzenia (UE) 2022/868.

(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 ***koordynatora danych i innych odnośnych*** właściwych organów ***oraz wszczynanie postępowań sądowych***. Organy te powinny być zobowiązane do współpracy, by skarga została właściwie rozpatrzona i ***szybko i skutecznie*** rozstrzygnięta. Aby skorzystać z mechanizmu 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 ([24]) oraz do dyrektywy Parlamentu Europejskiego i Rady (UE) 2020/1828 ([25]).

(83) Właściwe organy państw członkowskich powinny pilnować, by naruszenia obowiązków określonych w niniejszym rozporządzeniu podlegały karom. W tym celu powinny brać 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 uwzględniać to, czy sprawca naruszenia systematycznie lub w sposób powtarzający się nie wypełnia swoich obowiązków wynikających z niniejszego rozporządzenia. Aby pomóc przedsiębiorstwom w sporządzaniu 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 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.

([24]) 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).

([25]) 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).

(84) Aby wyeliminować ryzyko, że posiadacze ***baz danych zawierających dane uzyskane lub wygenerowane*** za pomocą elementów fizycznych, takich jak czujniki, produktów skomunikowanych i powiązanych usług***, w szczególności dane generowane maszynowo,*** będą powoływać się na prawo sui generis określone w art. 7 dyrektywy 96/9/WE***, niniejsze rozporządzenie precyzuje, że prawo*** sui generis ***nie ma zastosowania do takich baz danych, ponieważ nie byłyby spełnione wymogi ochrony istotnej inwestycji w uzyskanie, weryfikację lub prezentację danych zgodnie z art. 7 ust. 1 dyrektywy 96/9/WE***. ***Nie wpływa to na możliwe stosowanie*** prawa sui generis ***na podstawie art. 7 dyrektywy 96/9/WE względem*** baz danych ***zawierających dane niewchodzące w zakres niniejszego rozporządzenia, o ile są spełnione*** wymogi ochrony ***zgodnie z art. 7 ust. 1 tej dyrektywy***.

(85) Aby uwzględnić aspekty techniczne usług przetwarzania danych, należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 TFUE w odniesieniu do uzupełnienia niniejszego rozporządzenia w celu wprowadzenia mechanizmu monitorowania opłat z tytułu zmiany dostawcy nakładanych przez obecnych na rynku dostawców usług przetwarzania danych, doprecyzowania zasadniczych wymogów dotyczących interoperacyjności wobec ***uczestników*** przestrzeni danych***, którzy oferują dane lub usługi w zakresie danych innym uczestnikom***, 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 ([26]). 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, zmianom 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 słowników podstawowych interoperacyjności semantycznej, jak również w celu przyjęcia wspólnych specyfikacji dotyczących inteligentnych umów. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([27]).

(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 powiązań 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 interesu publicznego. Przepisy takie mogą obejmować dodatkowe wymogi dotyczące technicznych aspektów dostępu do danych, takich jak interfejsy dostępu do danych, lub sposobu zapewniania dostępu do danych, na przykład bezpośrednio przez produkt lub za pomocą usług 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 tworzenia 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.

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

([27]) 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).

(89) Aby umożliwić podmiotom gospodarczym dostosowanie się do nowych przepisów określonych w niniejszym rozporządzeniu ***i dokonać niezbędnych uzgodnień technicznych***, przepisy te powinny zacząć obowiązywać po ***18 miesiącach*** od wejścia rozporządzenia w życie. ***Obowiązki związane ze świadczeniem powiązanych usług w odniesieniu do produktów skomunikowanych już wprowadzonych do obrotu w ciągu ostatnich pięciu lat od wejścia w życie niniejszego rozporządzenia powinny mieć zastosowanie z mocą wsteczną wyłącznie w przypadku, gdy posiadacz danych i producent to ten sam podmiot. Takie obowiązki powinny być wypełniane tylko wówczas, gdy dostawca powiązanych usług jest w stanie zdalnie wdrożyć mechanizmy zapewniające spełnienie wymogów zgodnie z art. 1, i tylko wówczas, gdy wdrożenie takich mechanizmów nie stanowiłoby nieproporcjonalnego obciążenia dla producenta.***

(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:

a) takiego projektowania produktów skomunikowanych, by umożliwić dostęp do danych generowanych przez produkt skomunikowany lub generowanych w trakcie świadczenia użytkownikowi tego produktu powiązanych usług;

b) posiadaczy danych udostępniających dane pozyskane z produktu skomunikowanego lub wygenerowane w trakcie świadczenia powiązanej usługi osobom, których dane dotyczą, użytkownikom lub odbiorcom danych na wniosek użytkownika lub osoby, której dane dotyczą;

c) uczciwych warunków umownych dotyczących porozumień o udostępnianiu danych;

d) udostępniania danych organom sektora publicznego lub instytucjom, agencjom lub organom Unii w razie wystąpienia wyjątkowej potrzeby leżącej w interesie publicznym;

e) ułatwienia zmiany dostawcy usług przetwarzania danych;

f) wprowadzenia zabezpieczeń przed bezprawnym międzynarodowym dostępem administracji rządowej do danych nieosobowych; oraz

g) zapewnienia stworzenia norm i wspólnych specyfikacji w zakresie interoperacyjności na potrzeby przekazywanych i wykorzystywanych danych.

1a. Niniejsze rozporządzenie dotyczy danych osobowych i nieosobowych, w tym następujących rodzajów danych lub danych w następujących kontekstach:

a) rozdział II ma zastosowanie do dostępnych danych uzyskanych, zgromadzonych lub w inny sposób wygenerowanych przez produkty skomunikowane bądź wygenerowanych w trakcie świadczenia powiązanych usług;

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

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

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

e) rozdział VI ma zastosowanie do wszelkich danych i usług przetwarzanych w ramach usług przetwarzania danych;

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

2. Niniejsze rozporządzenie ma zastosowanie do:

a) producentów produktów ***skomunikowanych*** wprowadzanych do obrotu i ***dostawców*** powiązanych usług oferowanych w Unii***, niezależnie od miejsca siedziby,*** oraz użytkowników takich produktów ***skomunikowanych*** lub ***powiązanych*** usług ***lub – w przypadku danych osobowych – zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, do których odnoszą się dane pozyskane, zgromadzone lub wygenerowane w wyniku korzystania z tych produktów lub usług***;

b) ***użytkowników produktów skomunikowanych lub powiązanych usług w Unii oraz*** posiadaczy danych***, niezależnie od ich miejsca zamieszkania***, którzy udostępniają dane odbiorcom danych w Unii***, lub – w przypadku danych osobowych – zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, do których odnoszą się dane pozyskane, zgromadzone lub wygenerowane w wyniku korzystania z tych produktów lub usług***;

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

d) organów sektora publicznego ***państw członkowskich*** 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 ***konkretnego*** zadania realizowanego w interesie publicznym, oraz posiadaczy danych, którzy przekazują te dane w odpowiedzi na taki wniosek;

e) dostawców usług przetwarzania danych***, niezależnie od miejsca ich siedziby,*** oferujących takie usługi klientom w Unii.

3. Do ***wszelkich*** 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. ***Pozyskiwanie, gromadzenie lub generowanie danych osobowych w wyniku korzystania z produktu lub powiązanej usługi wymaga podstawy prawnej na mocy mającego zastosowanie prawa o ochronie danych.*** Niniejsze rozporządzenie ***nie stanowi podstawy prawnej dla przetwarzania danych osobowych. Niniejsze rozporządzenie nie narusza*** prawa Unii dotyczącego ochrony danych osobowych ***i prywatności***, w szczególności rozporządzenia (UE) 2016/679***, rozporządzenia (UE) 2018/1725*** i dyrektywy 2002/58/WE, w tym ***przepisów dotyczących uprawnień i kompetencji*** organów nadzorczych. ***W razie kolizji między niniejszym rozporządzeniem a prawem Unii dotyczącym ochrony danych osobowych lub prywatności lub prawem krajowym przyjętym zgodnie z takim prawem Unii pierwszeństwo ma odpowiednie prawo Unii lub prawo krajowe dotyczące ochrony danych osobowych i prywatności.*** 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 ***i uszczegóławiają*** prawo do przenoszenia danych określone w art. 20 rozporządzenia (UE) 2016/679. ***Żaden przepis niniejszego rozporządzenia nie może być stosowany ani interpretowany w sposób umniejszający lub ograniczający prawo do ochrony danych osobowych lub prawo do prywatności i poufności komunikacji.***

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 wykroczeń administracyjnych*** bądź wykonywania sankcji karnych ***lub kar administracyjnych***, w tym na rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 ([28]) 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, obronnością, bezpieczeństwem narodowym, administracją celną i podatkową oraz zdrowiem ***publicznym*** i bezpieczeństwem obywateli zgodnie z prawem Unii. ***Niniejsze rozporządzenie nie ma zastosowania do danych gromadzonych lub generowanych w kontekście działań związanych z obronnością lub przez produkty lub usługi związane z obronnością bądź przez produkty lub usługi wprowadzone i wykorzystywane do celów obronnych.***

4a. Niniejsze rozporządzenie uzupełnia prawo Unii służące wspieraniu interesów konsumentów i zapewnieniu wysokiego poziomu ochrony konsumentów, ochrony zdrowia konsumentów, ich bezpieczeństwa oraz ich interesów ekonomicznych, w tym dyrektywy 2005/29/WE, 2011/83/UE i 93/13/EWG, i nie wpływa na stosowanie tego prawa.

([28]) 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).

4b. Posiadacze danych nie są zobowiązani do udzielenia dostępu do danych żadnej osobie fizycznej lub prawnej, podmiotowi lub organowi spoza Unii, chyba że użytkownik złoży taki wniosek lub jest przewidziane w prawie Unii lub w krajowych przepisach wdrażających prawo Unii.

4c. Obowiązki określone w rozporządzeniu nie wykluczają dobrowolnej, zgodnej z prawem i uzgodnionej w umowach wzajemnej wymiany danych nieosobowych między użytkownikami, posiadaczami danych i odbiorcami danych.

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; ***treść lub dane uzyskane, wygenerowane lub zgromadzone przez produkt skomunikowany lub przekazane mu w imieniu innych osób w celu przechowywania lub przetwarzania, nie są objęte niniejszym rozporządzeniem.***

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

1b) „dane nieosobowe" oznaczają dane inne niż dane osobowe;

1c) „zgoda" oznacza zgodę zdefiniowaną w art. 4 pkt 11 rozporządzenia (UE) 2016/679;

1d) „osoba, której dane dotyczą" oznacza osobę, której dane dotyczą, zdefiniowaną w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

1e) „użytkownik danych" oznacza osobę fizyczną lub prawną, która ma zgodny z prawem dostęp do niektórych danych osobowych lub nieosobowych i ma prawo do wykorzystywania tych danych w celach komercyjnych lub niekomercyjnych;

2) „produkt ***skomunikowany***" oznacza ▌rzecz▌, która pozyskuje, generuje lub gromadzi ***dostępne*** dane dotyczące jej wykorzystania lub otoczenia, która jest w stanie przekazywać dane za pośrednictwem ***usługi*** łączności elektronicznej***, fizycznego łącza lub dostępu na urządzeniu*** i której podstawową funkcją nie jest przechowywanie, przetwarzanie ***ani przekazywanie*** danych ***w imieniu innych***;

3) „powiązana usługa" oznacza usługę cyfrową, w tym oprogramowanie, ***ale z wyłączeniem usług łączności elektronicznej,*** która jest wzajemnie połączona z produktem w taki sposób, że jej brak uniemożliwiłby produktowi wykonywanie ***co najmniej*** jednej z jego funkcji***, i która obejmuje uzyskanie dostępu do danych z produktu skomunikowanego przez dostawcę usługi***;

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 ***innych*** usług lub kontroluje ***funkcje produktów***;

4a) „konsument" oznacza każdą osobę fizyczną działającą w celach, które nie mieszczą się w ramach jej działalności handlowej, gospodarczej, rzemieślniczej lub zawodowej;

5) „użytkownik" oznacza osobę fizyczną lub prawną, która ***jest właścicielem produktu skomunikowanego, która korzysta z usługi powiązanej lub której właściciel produktu skomunikowanego przekazał, na podstawie umowy najmu lub leasingu, tymczasowe prawa do korzystania z produktu skomunikowanego lub z powiązanych usług, a jeżeli produkt skomunikowany lub powiązana usługa obejmuje przetwarzanie danych osobowych, użytkownik oznacza także osobę, której dane dotyczą***;

6) „posiadacz danych" oznacza osobę prawną lub fizyczną, która ***uzyskała dostęp do danych z produktu skomunikowanego lub wygenerowała dane w trakcie świadczenia usługi powiązanej i która ma przewidziane umową prawo do wykorzystywania takich danych oraz obowiązek*** udostępniania określonych danych ***użytkownikowi lub odbiorcy danych, zgodnie z niniejszym rozporządzeniem, mającym zastosowanie prawem Unii lub ustawodawstwem krajowym wdrażającym prawo Unii***;

7) „odbiorca danych" oznacza osobę prawną lub fizyczną ▌inną niż użytkownik produktu ***skomunikowanego*** lub powiązanej usługi, której to osobie posiadacz danych udostępnia dane, ***do których uzyskał dostęp z produktu skomunikowanego lub które wygenerował w trakcie świadczenia usługi powiązanej*** na ***wyraźny*** wniosek użytkownika ▌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 ***ograniczoną w czasie, taką jak stan zagrożenia zdrowia publicznego, sytuacja nadzwyczajna w wyniku klęski żywiołowej, a także poważna katastrofa spowodowana przez człowieka, w tym poważne cyberincydenty, która to sytuacja*** negatywnie ***wpływa*** na ludność Unii, państwa członkowskiego lub jego części ***i*** wiąże się z ryzykiem wystąpienia poważnych i trwałych następstw dla warunków życia lub stabilności gospodarczej, ***stabilności finansowej*** lub ***z ryzykiem*** znacznego ***i natychmiastowego*** obniżenia wartości aktywów gospodarczych w Unii lub w odpowiednim państwie członkowskim ***i którą stwierdza się i oficjalnie ogłasza zgodnie z odpowiednimi procedurami na mocy prawa Unii lub prawa krajowego***;

10a) „oficjalne statystyki" oznaczają „statystykę europejską" w rozumieniu rozporządzenia (WE) nr 223/2009 ([29]);

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 ***standardy***" oznaczają specyfikacje techniczne ▌, które są ukierunkowane na osiągnięcie interoperacyjności między usługami przetwarzania danych ***i które są przyjmowane w drodze inkluzywnego, opartego na współpracy i konsensusie oraz przejrzystego procesu, z którego nie można wykluczyć podmiotów, których ta kwestia istotnie dotyczy, ani zainteresowanych stron***;

▌

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

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

19) „interoperacyjność” oznacza zdolność co najmniej dwóch ***usług opartych na danych, w tym*** przestrzeni danych, sieci komunikacyjnych, systemów, aplikacji lub komponentów do ***przetwarzania,*** wymiany i wykorzystywania danych w celu wykonywania swoich funkcji ***w sposób dokładny, efektywny i konsekwentny***;

19a) „możliwość przenoszenia”’ oznacza zdolność klienta do przenoszenia zaimportowanych lub bezpośrednio wygenerowanych danych, które można jednoznacznie przypisać do klienta, pomiędzy jego własnym systemem a usługami w chmurze oraz pomiędzy usługami w chmurze różnych dostawców usług w chmurze;

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

20a) „wspólne europejskie przestrzenie danych” oznaczają interoperacyjne ramy wspólnych norm i praktyk, specyficzne dla danego celu lub sektora bądź międzysektorowe, w których odbywa się wymiana lub wspólne przetwarzanie danych na potrzeby m.in. opracowywania nowych produktów i usług, badań naukowych lub inicjatyw społeczeństwa obywatelskiego.

20b) „metadane” oznaczają ustrukturyzowany opis treści danych ułatwiający wyszukiwanie lub wykorzystywanie tych danych;

20c) „usługa pośrednictwa w zakresie danych” oznacza usługę pośrednictwa w zakresie danych zdefiniowaną w art. 2 pkt 8 rozporządzenia (UE) 2022/868;

20d) „altruizm danych” oznacza dobrowolne dzielenie się danymi zdefiniowane w art. 2 pkt 16 rozporządzenia (UE) 2022/868;

20e) „tajemnica przedsiębiorstwa” oznacza informacje spełniające wszystkie wymogi art. 2 pkt 1 dyrektywy (UE) 2016/943;

20f) „posiadacz tajemnicy przedsiębiorstwa” oznacza posiadacza tajemnicy przedsiębiorstwa zdefiniowanego w art. 2 pkt 2 dyrektywy (UE) 2016/943.

ROZDZIAŁ II

UDOSTĘPNIANIE DANYCH PRZEZ PRZEDSIĘBIORSTWA KONSUMENTOM I MIĘDZY PRZEDSIĘBIORSTWAMI

Artykuł 3

Obowiązek udostępniania ***użytkownikowi*** danych***, do których uzyskano dostęp z produktów skomunikowanych lub które wygenerowano podczas świadczenia*** powiązanych usług

1. Produkty ***skomunikowane*** projektuje się i wytwarza ***w taki sposób, aby dane przez nie gromadzone, generowane lub w inny sposób uzyskiwane, które są dostępne dla posiadaczy danych lub odbiorców danych,*** były domyślnie ***bezpłatne dla użytkownika oraz*** łatwo, bezpiecznie oraz – w stosownych przypadkach ***i jeżeli jest to technicznie wykonalne*** – bezpośrednio ***mu*** dostępne***, w zrozumiałej i uporządkowanej formie, w powszechnie używanym formacie nadającym się do odczytu maszynowego. Dane udostępnia się w formie, w jakiej zostały zgromadzone, uzyskane lub wygenerowane przez produkt skomunikowany, z minimalnymi dostosowaniami niezbędnymi, aby umożliwić ich wykorzystanie przez osobę trzecią, w tym wraz z powiązanymi metadanymi niezbędnymi do interpretacji i wykorzystania danych. Informacji wywiedzionych lub wywnioskowanych z tych danych za pomocą złożonych algorytmów własnościowych, w szczególności gdy łączą one dane wyjściowe z wielu czujników w produkcie skomunikowanym, nie uznaje się za wchodzące w zakres obowiązku posiadacza danych do udostępnienia danych użytkownikom lub odbiorcom danych, chyba że użytkownik i posiadacz danych uzgodnią inaczej. Jeżeli użytkownik jest osobą, której dane dotyczą, produkty skomunikowane oferują możliwość bezpośredniego wykonywania praw osób, których dane dotyczą, jeżeli jest to technicznie wykonalne. Produkty skomunikowane projektuje się i wytwarza w taki sposób, aby osoba, której dane dotyczą, niezależnie od tytułu prawnego do produktu skomunikowanego, miała możliwość korzystania z produktów objętych niniejszym rozporządzeniem w sposób jak najmniej naruszający prywatność. Wymogi określone w akapicie pierwszym należy spełnić bez zakłócania funkcjonalności produktu skomunikowanego i powiązanych usług oraz zgodnie z wymogami w zakresie bezpieczeństwa danych określonymi w prawie Unii.***

1a. Posiadacze danych mogą odrzucić wniosek o udostępnienie danych, jeżeli dostęp do danych jest zakazany przez prawo Unii lub prawo krajowe.

2. Przed zawarciem umowy dotyczącej zakupu ***produktu skomunikowanego producent lub, w stosownych przypadkach, sprzedawca przekazuje użytkownikowi*** co najmniej następujące informacje ***w sposób prosty oraz*** w jasnym i zrozumiałym formacie:

a) ***rodzaj danych, format, częstotliwość próbkowania, pojemność pamięci urządzenia oraz szacunkową*** ilość ***dostępnych*** danych***, które produkt skomunikowany może zgromadzić, wygenerować lub w inny sposób uzyskać***;

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

ba) czy dane będą przechowywane na urządzeniu czy na zdalnym serwerze i przez jaki okres;

c) w jaki sposób użytkownik może uzyskać ***bezpłatny*** dostęp do tych danych***, pobrać je i wystąpić o ich usunięcie***;

ca) techniczne środki dostępu do danych, takie jak zestawy SDK czy interfejsy programowania aplikacji, oraz warunki ich użytkowania i jakość usługi muszą być opisane w stopniu wystarczającym, aby umożliwić opracowanie takich środków dostępu;

cb) czy posiadacz danych jest posiadaczem tajemnic przedsiębiorstwa lub innych praw własności intelektualnej związanych z danymi, do których można uzyskać dostęp z produktu skomunikowanego lub które mogą być generowane w trakcie świadczenia powiązanej usługi, a jeśli nie, jaka jest tożsamość posiadacza tajemnic przedsiębiorstwa, np. jego nazwa handlowa i adres fizyczny, pod którym ma siedzibę;

▌

2a. Powiązane usługi muszą być świadczone w taki sposób, aby dane wygenerowane w trakcie ich świadczenia, które odzwierciedlają cyfryzację czynności lub zdarzeń użytkownika, były bezpłatne dla użytkownika oraz domyślnie łatwo, bezpiecznie i, w stosownych przypadkach i jeżeli jest to technicznie wykonalne, bezpośrednio dostępne dla użytkownika w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, wraz z odpowiednimi metadanymi niezbędnymi do ich interpretacji i wykorzystania.

2b. Zanim użytkownik zawrze umowę z dostawcą usług powiązanych, która obejmuje dostęp dostawcy do danych z produktu skomunikowanego podczas świadczenia takich usług, zgodnie z art. 4 ust. 6 niniejszego rozporządzenia, umowa musi zawierać następujące elementy:

a) informacje na temat charakteru, ilości, częstotliwości gromadzenia i formatu danych z produktu skomunikowanego dostępnych dostawcy usług powiązanych oraz, w stosownych przypadkach, warunki dostępu użytkownika do takich danych lub ich pobierania, w tym okres ich przechowywania;

b) informacje na temat charakteru i szacunkowej ilości danych generowanych w trakcie świadczenia usługi powiązanej, a także warunki dostępu użytkownika do takich danych lub ich pobierania;

c) szczegółowe opcje wyrażenia świadomej zgody na przetwarzanie danych w rozumieniu art. 4 pkt 11 rozporządzenia (UE) 2016/679;

d) informację, czy dostawca usług świadczący usługę powiązaną, działając w charakterze posiadacza danych, zamierza sam wykorzystywać dane, do których uzyska dostęp z produktu skomunikowanego, czy też zezwolić co najmniej jednej osobie trzeciej na wykorzystywanie tych danych do celów uzgodnionych z użytkownikiem;

e) nazwę handlową dostawcy usługi powiązanej, jego identyfikator podmiotu prawnego, dane kontaktowe i adres geograficzny, pod którym ma siedzibę, oraz, w stosownych przypadkach, informacje na temat innych stron przetwarzających dane;

f) w stosownych przypadkach – informacje na temat środków komunikacji umożliwiających użytkownikowi szybki kontakt z dostawcą i sprawną komunikację z jego pracownikami;

g) informację, w jaki sposób użytkownik może zażądać udostępnienia danych odbiorcy danych i wycofać zgodę na udostępnianie danych;

h) informację, czy posiadacz danych jest posiadaczem tajemnic przedsiębiorstwa lub innych praw własności intelektualnej związanych z danymi, do których można uzyskać dostęp z produktu skomunikowanego lub które mogą być generowane w trakcie świadczenia powiązanej usługi, a jeśli nie, jaka jest tożsamość posiadacza tajemnic przedsiębiorstwa, np. jego nazwa handlowa, identyfikator podmiotu prawnego i adres geograficzny, pod którym ma siedzibę;

i) informację, jak użytkownik może zarządzać zezwoleniami na korzystanie z danych, najlepiej ze szczegółowymi wariantami zezwolenia, a także z możliwością cofnięcia zezwoleń na korzystanie z danych użytkownika posiadaczowi danych lub osobom trzecim wyznaczonym przez posiadacza danych, lub z możliwością wykluczenia adresów geograficznych;

j) okres obowiązywania umowy między użytkownikiem a dostawcą usługi powiązanej, jak również sposoby przedwczesnego rozwiązania takiej umowy, a także minimalny okres, przez który gwarantuje się aktualizacje bezpieczeństwa i funkcjonalności powiązanej usługi;

k) prawo użytkownika do wniesienia skargi w związku z naruszeniem przepisów niniejszego rozdziału do koordynatora danych, o którym mowa w art. 31.

Artykuł 3a

Umiejętność korzystania z danych

1. Wdrażając niniejsze rozporządzenie, Unia i państwa członkowskie wspierają środki i narzędzia służące rozwijaniu umiejętności korzystania z danych we wszystkich sektorach i z uwzględnieniem różnych potrzeb grup użytkowników, konsumentów i przedsiębiorstw, w tym przez kształcenie i szkolenie, programy podnoszenia kwalifikacji i przekwalifikowania, z zachowaniem odpowiedniej równowagi płci i wieku, by umożliwić powstanie sprawiedliwego społeczeństwa opartego na danych i rynku danych.

Artykuł 4

Prawa i obowiązki użytkowników ***i posiadaczy danych w zakresie*** dostępu do danych ***pochodzących z produktów skomunikowanych lub*** wygenerowanych ***w trakcie świadczenia*** usług powiązanych ***oraz w zakresie korzystania z tych danych i udostępniania ich***

1. Jeżeli użytkownik nie może uzyskać bezpośredniego dostępu do danych z produktu, ***posiadacze*** danych ***udostępniają*** użytkownikowi bez zbędnej zwłoki ***wszelkie*** dane ***pozyskane przez nich z produktu skomunikowanego lub*** wygenerowane ***w trakcie świadczenia usługi powiązanej, w sposób łatwy i bezpieczny, w zrozumiałej i uporządkowanej formie, w powszechnie używanym formacie nadającym się do odczytu maszynowego, nieodpłatnie oraz, w stosownych przypadkach i*** jeżeli jest to technicznie wykonalne, w sposób ciągły i w czasie rzeczywistym***, w tym udostępnia dane osobowe pochodzące z takich danych osobie, której dane dotyczą, zgodnie z art. 15 rozporządzenia (UE) 2016/679, wraz z odpowiednimi metadanymi. Dane dostarcza się w formie, w jakiej zostały pobrane z produktu skomunikowanego lub wygenerowane przez usługę powiązaną, z minimalnymi dostosowaniami niezbędnymi, aby umożliwić ich wykorzystanie przez osobę trzecią, w tym z powiązanymi metadanymi niezbędnymi do interpretacji i wykorzystania danych. Informacji wywiedzionych lub wywnioskowanych z tych danych za pomocą złożonych algorytmów własnościowych, w szczególności gdy łączą one dane wyjściowe z wielu czujników w produkcie skomunikowanym, nie uznaje się za wchodzące w zakres obowiązku posiadacza danych do udostępniania danych użytkownikom lub odbiorcom danych, chyba że użytkownik i posiadacz danych uzgodnią inaczej. Wszelkie wnioski o dostęp do danych kierowane do posiadacza danych powinny być składane za pomocą*** zwykłego wniosku drogą elektroniczną, jeżeli jest to technicznie wykonalne***, oraz, w stosownych przypadkach, wskazywać rodzaj, charakter lub zakres żądanych danych***.

1a. Posiadacze danych mogą odrzucić wniosek o udostępnienie danych, jeżeli dostęp do danych jest zakazany przez prawo Unii lub prawo krajowe.

1b. Użytkownicy i posiadacze danych mogą uzgodnić umownie ograniczenie lub zakaz dostępu do danych, ich wykorzystywania lub dalszego udostępniania, jeżeli mogłoby to zagrozić bezpieczeństwu produktu określonemu w przepisach prawa. Każda ze stron może przekazać sprawę koordynatorowi danych, aby ocenić, czy takie ograniczenie jest uzasadnione, w szczególności w świetle poważnego negatywnego wpływu na zdrowie, bezpieczeństwo lub ochronę ludzi. Właściwe organy sektorowe będą miały możliwość zapewnienia fachowej wiedzy technicznej w tym kontekście.

1c. Jeżeli przestrzegane są wszystkie przepisy ustanowione w niniejszym rozporządzeniu oraz warunki uzgodnione w umowie między stronami, posiadacz danych nie ponosi odpowiedzialności wobec użytkownika za żadne szkody wynikające z udostępnionych danych, pod warunkiem że posiadacz danych przetwarza dane zgodnie z prawem Unii i prawem krajowym oraz spełnia odpowiednie wymogi w zakresie cyberbezpieczeństwa, a w stosownych przypadkach stosuje środki techniczne i organizacyjne mające na celu zachowanie poufności udostępnianych danych. Wypełniając

przepisy niniejszego rozporządzenia, użytkownik, który zgodnie z prawem udostępnia osobie trzeciej dane, do których uzyskał dostęp z produktu skomunikowanego lub które otrzymał w następstwie wniosku złożonego na podstawie art. 4 ust. 1, lub odbiorca danych, lub który zgodnie z prawem udostępnia osobie trzeciej dane udostępnione mu przez posiadacza danych, nie ponosi odpowiedzialności za szkody wynikające z udostępniania takich danych, pod warunkiem że użytkownik lub odbiorca danych przetwarza dane zgodnie z prawem Unii i prawem krajowym oraz spełnia odpowiednie wymogi w zakresie cyberbezpieczeństwa, a w stosownych przypadkach stosuje środki techniczne i organizacyjne mające na celu zachowanie poufności udostępnianych danych.

1d. Posiadacze danych nie utrudniają nadmiernie egzekwowania praw i dokonywania wyborów przez użytkowników, w tym poprzez oferowanie użytkownikom wyboru w nieneutralny sposób, ani też nie podważają ani nie ograniczają autonomii, zdolności decyzyjnej ani swobody wyboru użytkowników za pomocą struktury, funkcji lub sposobu zaprojektowania i działania interfejsu użytkownika bądź jego elementów.

2. ***Posiadacze*** danych nie ***wymagają*** od użytkownika podawania żadnych informacji poza tymi, które są konieczne do zweryfikowania, czy jest on użytkownikiem zgodnie z ust. 1. ***Posiadacze*** danych nie ***mogą*** 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. ***W przypadku gdy identyfikacja jest wymagana prawem, posiadacze danych umożliwiają użytkownikom identyfikację i uwierzytelnienie za pośrednictwem europejskich portfeli tożsamości cyfrowej na podstawie rozporządzenia (UE) nr 910/2014.***

3. Tajemnice przedsiębiorstwa ***chroni się i*** ujawnia wyłącznie pod warunkiem ***uprzedniego*** zastosowania ***zgodnie z dyrektywą UE 2016/943*** wszelkich szczególnych środków niezbędnych do zachowania ***ich*** poufności ▌, w szczególności w odniesieniu do osób trzecich. Posiadacz danych ***lub posiadacz tajemnicy przedsiębiorstwa, jeśli nie jest to jednocześnie posiadacz danych, identyfikuje dane chronione jako tajemnice przedsiębiorstwa i może*** uzgodnić ***z użytkownikiem wszelkie*** środki ***techniczne i organizacyjne*** mające na celu zachowanie poufności udostępnianych danych, w szczególności w odniesieniu do osób trzecich***, a także przepisy o odpowiedzialności. Takie środki techniczne i organizacyjne obejmują w stosownych przypadkach modelowe postanowienia umowne, umowy o poufności, ścisłe protokoły dostępu, standardy techniczne i stosowanie kodeksów postępowania. Jeżeli użytkownik nie stosuje tych środków lub narusza poufność tajemnic przedsiębiorstwa, posiadacz danych może zawiesić udostępnianie danych zidentyfikowanych jako tajemnice przedsiębiorstwa. W takich przypadkach posiadacz danych niezwłocznie powiadamia koordynatora danych państwa członkowskiego, w którym ma siedzibę, zgodnie z art. 31 niniejszego rozporządzenia, że zawiesił udostępnianie danych, i wskazuje, których środków nie zastosowano lub które tajemnice przedsiębiorstwa naruszono. Jeżeli użytkownik chce zaskarżyć decyzję posiadacza danych o zawieszeniu udostępniania danych, koordynator danych decyduje w rozsądnym terminie, czy dane mają być ponownie udostępnione, a jeżeli tak, to na jakich warunkach.***

4. Użytkownik nie może wykorzystywać danych uzyskanych na podstawie wniosku, o którym mowa w ust. 1, do opracowania produktu konkurującego ***bezpośrednio*** z produktem, z którego pochodzą dane***, lub z jego częścią i nie może wykorzystywać takich danych do uzyskania informacji na temat sytuacji gospodarczej producenta, jego aktywów i metod produkcji***.

4a. Użytkownik nie może w celu uzyskania dostępu do danych stosować przymusu ani wykorzystywać luk w infrastrukturze technicznej posiadacza danych mającej chronić dane.

4b. Użytkownicy mają prawo do udostępniania danych nieosobowych pozyskanych z produktu skomunikowanego lub na podstawie wniosku, o którym mowa w ust. 1, każdemu odbiorcy danych w celach komercyjnych lub niekomercyjnych, bezpośrednio lub za pośrednictwem posiadacza danych lub dostawców usług pośrednictwa w zakresie danych, jak określono w rozporządzeniu (UE) 2022/868. Udostępnianie danych między użytkownikiem a odbiorcą danych odbywa się na podstawie umów; przepisy rozdziału IV dotyczące uczciwych, rozsądnych i niedyskryminacyjnych warunków stosuje się odpowiednio do umów między użytkownikami a odbiorcami danych.

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 ***spełnione są wszystkie warunki i przestrzegane są wszystkie przepisy przewidziane w mającym zastosowanie prawie o ochronie danych, w szczególności gdy*** istnieje ważna podstawa prawna zgodnie z art. ***6*** rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, spełnione są warunki określone w art. 9 rozporządzenia (UE) 2016/679 ***i w art. 5 ust. 3 dyrektywy 2002/58/WE***.

6. ***Posiadacze danych wykorzystują*** wszelkie dane nieosobowe ***uzyskane ze skomunikowanego produktu lub*** wygenerowane ***w trakcie świadczenia*** powiązanej usługi wyłącznie na podstawie umowy z użytkownikiem. Posiadacz danych nie ***uzależnia możliwości korzystania z produktu lub powiązanej usługi od tego, czy użytkownik zezwoli mu na przetwarzanie danych niewymaganych do funkcjonowania produktu lub świadczenia powiązanej usługi. Posiadacz danych usuwa dane, gdy nie są już one niezbędne do celu uzgodnionego w umowie. Posiadacze*** danych ***i użytkownicy*** nie ***mogą*** wykorzystywać takich danych ***pozyskanych, zgromadzonych lub*** wygenerowanych w wyniku korzystania z produktu lub powiązanej usługi do pozyskania informacji na temat sytuacji ekonomicznej, aktywów i metod produkcji ***drugiej strony*** lub korzystania ***z produktu lub powiązanej usługi*** przez ***drugą stronę***, które to informacje mogłyby osłabić pozycję handlową ***drugiej strony*** na rynkach, na których prowadzi ***ona*** działalność.

6a. Posiadacze danych nie mogą udostępniać danych nieosobowych pozyskanych z produktu skomunikowanego, o których mowa w art. 3 ust. 2, osobom trzecim do celów komercyjnych lub niekomercyjnych innych niż wypełnianie ich obowiązków umownych wobec użytkownika. W stosownych przypadkach posiadacze danych umownie zobowiązują strony trzecie, by nie udostępniały dalej otrzymanych od nich danych.

6b. W przypadku gdy umowa między użytkownikiem a posiadaczem danych zezwala na wykorzystanie danych nieosobowych pozyskanych przez nich z produktu skomunikowanego, o których mowa w art. 3 ust. 2a lit. a), posiadacz danych ma możliwość wykorzystania tych danych do któregokolwiek z następujących celów:

a) poprawy funkcjonowania produktu skomunikowanego lub powiązanych z nim usług;

b) opracowywania nowych produktów lub usług;

c) wzbogacania ich lub manipulowania nimi lub agregowania ich z innymi danymi, w tym w celu udostępnienia powstałego zbioru danych osobom trzecim, o ile taki pochodny zbiór danych nie pozwala na identyfikację konkretnych elementów danych przekazanych posiadaczowi danych z produktu skomunikowanego lub nie pozwala osobie trzeciej na wywnioskowanie tych elementów danych ze zbioru danych.

6c. Użytkownicy w relacjach między przedsiębiorstwami mają prawo do udostępniania danych odbiorcom danych lub posiadaczom danych na podstawie wszelkich zgodnych z prawem warunków umownych, w tym poprzez uzgodnienie ograniczenia lub limitu dalszego udostępniania takich danych, oraz do otrzymania proporcjonalnego wynagrodzenia w zamian za rezygnację z przysługującego im prawa do zgodnego z prawem wykorzystywania lub udostępniania takich danych. Odbiorcy danych lub posiadacze danych nie mogą uzależniać oferty powiązanych usług lub warunków handlowych, w tym cen, od takiej zgody użytkownika, ani zmuszać go, wprowadzać w błąd lub manipulować nim w jakikolwiek inny sposób w celu udostępnienia danych na takich warunkach umownych.

Artykuł 5

Prawo ***użytkownika*** do udostępniania danych osobom trzecim

1. Na wniosek użytkownika lub strony działającej w jego imieniu***, takiej jak upoważniony dostawca usług pośrednictwa danych w rozumieniu rozporządzenia (UE) 2022/868, posiadacze danych udostępniają*** osobie trzeciej – bez zbędnej zwłoki***, w sposób łatwy i bezpieczny, w zrozumiałej i uporządkowanej formie, w powszechnie używanym formacie nadającym się do odczytu maszynowego, nieodpłatnie dla użytkownika oraz, w stosownych przypadkach i jeżeli jest to technicznie wykonalne, w sposób ciągły i w czasie rzeczywistym – dane pozyskane przez nich z produktu skomunikowanego lub wygenerowane w trakcie świadczenia usługi powiązanej o takiej samej jakości, jaka jest dostępna posiadaczowi danych. Jeżeli użytkownik jest osobą, której dane dotyczą, dane osobowe są przetwarzane do celów określonych przez osobę, której dane dotyczą, takich jak:***

a) świadczenie usług na rynkach niższego szczebla, takich jak konserwacja i naprawa produktu, w tym usług konkurujących z produktem skomunikowanym lub usługą świadczoną przez posiadacza danych;

b) umożliwienie użytkownikowi aktualizacji oprogramowania produktu skomunikowanego lub powiązanych usług, w szczególności w celu rozwiązania problemów związanych z bezpieczeństwem i użytecznością;

c) określone usługi pośrednictwa w zakresie danych uznane w Unii lub specjalne usługi świadczone przez uznane w Unii organizacje altruizmu danych zgodnie z warunkami i wymogami rozdziałów III i IV rozporządzenia (UE) 2022/868.

Dane dostarcza się w formacie, w jakim zostały pozyskane z produktu, z minimalnymi dostosowaniami niezbędnymi, aby umożliwić ich wykorzystanie przez osobę trzecią, łącznie z powiązanymi metadanymi niezbędnymi do interpretacji i wykorzystania danych. Informacji wywiedzionych lub wywnioskowanych z tych danych za pomocą złożonych algorytmów własnościowych, w szczególności gdy łączą one dane wyjściowe z wielu czujników w produkcie skomunikowanym, nie uznaje się za wchodzące w zakres obowiązku posiadacza danych do udostępniania danych użytkownikom lub odbiorcom danych, chyba że użytkownik i posiadacz danych uzgodnią inaczej.

1a. Prawo na mocy ust. 1 nie ma zastosowania do danych wynikających z korzystania z produktu lub powiązanej usługi w kontekście testowania innych nowych produktów, substancji lub procesów, które nie zostały jeszcze wprowadzone do obrotu, chyba że korzystanie przez osobę trzecią jest dozwolone na podstawie umowy z przedsiębiorstwem, z którym użytkownik uzgodnił wykorzystywanie jednego ze swoich produktów do testowania innych nowych produktów, substancji lub procesów.

2. Żadne przedsiębiorstwo świadczące podstawowe usługi platformowe, w przypadku którego co najmniej jedną z takich usług wyznaczono jako strażnika dostępu na podstawie art. […] rozporządzenia ***(UE) 2022/1925***, nie może być kwalifikującym się ***odbiorcą danych*** 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;

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

3. Użytkownik lub ***odbiorca danych*** nie są zobowiązani do podawania żadnych informacji poza tymi, które są konieczne do zweryfikowania, czy są oni użytkownikiem lub ***odbiorcą danych*** zgodnie z ust. 1. ***Posiadacze*** danych nie ***mogą*** przechowywać żadnych informacji na temat dostępu ***odbiorcy danych*** do żądanych danych poza informacjami, które są niezbędne do należytego wykonania wniosku ***odbiorcy danych*** o uzyskanie dostępu oraz do bezpieczeństwa i utrzymania infrastruktury danych.

4. ***Odbiorca danych*** nie może stosować środków przymusu ani nadużywać ▌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 ***pozyskanych, zgromadzonych lub*** 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 ***jednoznacznie*** wyrazi zgodę na takie wykorzystanie i ma techniczną możliwość ***łatwego*** wycofania tej zgody w dowolnym momencie.

6. ***W przypadku gdy osoba***, której dane dotyczą, ***nie jest użytkownikiem występującym z wnioskiem o udzielenie dostępu,*** wszelkie dane osobowe ***pozyskane, zgromadzone lub*** wygenerowane w wyniku korzystania ***przez niego*** z produktu lub powiązanej usługi ***oraz dane wywiedzione lub wywnioskowane w wyniku tego korzystania*** są udostępniane ***osobie trzeciej przez posiadacza danych*** wyłącznie wtedy, gdy istnieje ważna podstawa prawna zgodnie z art. ***6*** rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, spełnione są warunki określone w art. 9 rozporządzenia (UE) 2016/679 ***i w art. 5 ust. 3 dyrektywy 2002/58/WE***.

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 ***wniosku*** uzgodnionego między użytkownikiem a osobą trzecią, a osoba trzecia ***przed ujawnieniem*** stosuje wszystkie szczególne niezbędne środki uzgodnione między posiadaczem danych – ***lub między posiadaczem tajemnic przedsiębiorstwa, jeśli nie jest on jednocześnie posiadaczem danych*** – a osobą trzecią w celu zachowania poufności tajemnicy przedsiębiorstwa. W takim przypadku ***posiadacz danych lub posiadacz tajemnicy przedsiębiorstwa wskazuje dane chronione jako tajemnice*** przedsiębiorstwa oraz ***techniczne i organizacyjne*** środki służące zachowaniu

poufności***, a także przepisy dotyczące odpowiedzialności. Takie środki techniczne i organizacyjne*** określa się w umowie między posiadaczem danych ***lub posiadaczem tajemnicy przedsiębiorstwa*** a stroną trzecią***, a obejmują one w stosownych przypadkach modelowe postanowienia umowne, ścisłe protokoły dostępu, umowy o poufności, standardy techniczne i stosowanie kodeksów postępowania. Jeżeli osoby trzecia nie stosuje tych środków lub narusza poufność tajemnic przedsiębiorstwa, posiadacz danych może zawiesić udostępnianie danych wskazanych jako tajemnice przedsiębiorstwa. W takich przypadkach posiadacz danych musi niezwłocznie powiadomić koordynatora danych państwa członkowskiego, w którym ma siedzibę, zgodnie z art. 31, że zawiesił udostępnianie danych, i wskazuje, których środków nie zastosowano lub które tajemnice przedsiębiorstwa naruszono. Jeżeli osoba trzecia chce zaskarżyć decyzję posiadacza danych o zawieszeniu udostępniania danych, koordynator danych decyduje w rozsądnym terminie, czy dane mają być ponownie udostępnione, a jeżeli tak, to na jakich warunkach.***

9. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa ***osób, których dane dotyczą, zgodnie z mającym zastosowanie prawem o ochronie*** danych.

Artykuł 6

Obowiązki ***odbiorców danych*** otrzymujących dane na wniosek użytkownika

1. ***Odbiorca danych*** przetwarza dane udostępnione ***mu*** na podstawie art. 5 wyłącznie do celów ***i na warunkach uzgodnionych z użytkownikiem i jeżeli spełnione są wszystkie warunki i przestrzegane są wszystkie przepisy przewidziane w mającym zastosowanie prawie o ochronie danych, zwłaszcza 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 i w art. 5 ust. 3 dyrektywy 2002/58/WE,*** i z zastrzeżeniem praw osoby, której dane dotyczą, w odniesieniu do danych osobowych***. Odbiorca danych*** usuwa dane, gdy nie są już one niezbędne do uzgodnionego celu***, chyba że uzgodniono inaczej z użytkownikiem***.

2. ***Odbiorca danych*** nie może:

a) ***nadmiernie utrudniać egzekwowania praw i wyborów przez użytkowników, w tym przez oferowanie użytkownikom wyboru w nieneutralny sposób,*** w żaden sposób zmuszać ani oszukiwać użytkownika ani też nim manipulować***, bądź podważać lub ograniczać*** autonomii, zdolności decyzyjnej lub wyborów użytkownika, w tym za pomocą interfejsu cyfrowego z użytkownikiem ***lub jego części, jak również jego struktury, sposobu zaprojektowania, funkcji lub sposobu obsługi***;

b) wykorzystywać otrzymanych danych do profilowania osób fizycznych w rozumieniu art. 4 pkt 4 rozporządzenia (UE) 2016/679 ***w sposób inny niż zgodny z tym rozporządzeniem***;

c) udostępniać otrzymanych danych innej osobie trzeciej ***bez informowania użytkownika w jasny i łatwo dostępny sposób oraz bez zwracania się do użytkownika o wyraźną zgodę umowną***;

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. ***[3 rozporządzenia (UE) 2022/1925*** (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; ***odbiorcy danych nie mogą również wykorzystywać żadnych danych nieosobowych wygenerowanych w wyniku korzystania z produktu lub powiązanej usługi do pozyskania informacji na temat sytuacji ekonomicznej, aktywów i metod produkcji posiadacza danych lub korzystania przez posiadacza danych, które to informacje mogłyby osłabić pozycję handlową posiadacza danych na rynkach, na których prowadzi działalność;***

ea) wykorzystywać otrzymanych danych w sposób, który odbija się na bezpieczeństwie produktu lub powiązanych usług;

eb) w stosownych przypadkach – ignorować szczególnych środków uzgodnionych z posiadaczem danych lub posiadaczem tajemnic przedsiębiorstwa zgodnie z art. 5 ust. 8 niniejszego rozporządzenia oraz naruszać poufności tajemnic przedsiębiorstwa;

ec) wykorzystywać danych w celu zakłócenia szczególnie chronionych informacji dotyczących ochrony infrastruktury krytycznej w rozumieniu art. 2 lit. d) dyrektywy 2008/114/WE.

▌

2a. Osoba trzecia odpowiada za zapewnienie bezpieczeństwa i ochrony danych, które otrzymuje od posiadacza danych.

Artykuł 7

Zakres obowiązków udostępniania danych przez przedsiębiorstwa konsumentom i między przedsiębiorstwami

1. Obowiązki określone w niniejszym rozdziale nie mają zastosowania do ***przedsiębiorstw***, 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***, i gdy to mikroprzedsiębiorstwo i małe przedsiębiorstwo nie jest podwykonawcą, któremu zlecono wytworzenie lub zaprojektowanie produktu lub też świadczenie usługi powiązanej***.

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 ***uzgodnić z odbiorcą danych sposób udostępniania danych i*** czynić to na sprawiedliwych, rozsądnych i niedyskryminujących warunkach oraz w przejrzysty sposób zgodnie z przepisami niniejszego rozdziału i rozdziału IV.

2. ▌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 ***w sposobie udostępniania danych*** 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 ***ma uzasadnione podejrzenia***, że warunki, na jakich dane zostały mu udostępnione, są dyskryminujące, ***posiadacz danych bezzwłocznie dostarcza odbiorcy danych dowody wykazujące***, że nie doszło do dyskryminacji.

▌

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.

5a. Posiadacze danych i odbiorcy danych podejmują wszelkie niezbędne środki prawne, organizacyjne i techniczne, by zapewnić bezpieczeństwo i integralność transferów danych.

6. O ile prawo Unii, w tym art. ***4 ust. 3, art. 5 ust. 8 i 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 ***w relacjach między przedsiębiorstwami*** musi być ***niedyskryminacyjne i*** rozsądne. ***Posiadacz danych, odbiorca danych ani strona trzecia nie mogą bezpośrednio ani pośrednio pobierać od konsumentów lub osób, których dane dotyczą, opłaty, wynagrodzenia lub kosztów z tytułu udostępnienia danych lub zapewnienia dostępu do danych.***

2. W przypadku gdy odbiorcą danych jest ***organizacja badawcza nienastawiona na zysk lub MŚP*** zgodnie z definicją w art. 2 załącznika do zalecenia 2003/361/WE ***i pod warunkiem, że te przedsiębiorstwa nie mają przedsiębiorstw partnerskich ani przedsiębiorstw powiązanych zdefiniowanych w art. 3 załącznika do zalecenia 2003/361/WE i nie kwalifikują się jako MŚP,*** 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. ***W przypadku MŚP posiadacz danych aktywnie informuje o obowiązku dostarczenia danych, najlepiej na podstawie modelu opartego na kosztach.***

2a. Komisja opracuje wytyczne w celu określenia kryteriów dla kategorii kosztów związanych z udostępnianiem danych, które stanowią podstawę przyznania wynagrodzenia zgodnie z ust. 1.

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. ***Użytkownicy,*** posiadacze danych i odbiorcy danych mają dostęp do organów rozstrzygania sporów, certyfikowanych zgodnie z ust. 2 niniejszego artykułu, na potrzeby rozstrzygania sporów dotyczących ***wypełniania przez posiadacza danych obowiązku udostępniania danych odbiorcy danych na wniosek użytkownika,*** ustalania sprawiedliwych, rozsądnych i niedyskryminujących warunków udostępniania danych oraz przejrzystego sposobu udostępniania danych zgodnie z art. 8***, 9*** i 13.

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 ***państwa członkowskiego, w którym ma siedzibę***.

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.

7a. Organy rozstrzygania sporów przekazują do wiadomości publicznej roczne sprawozdania z działalności. Każde roczne sprawozdanie zawiera w szczególności następujące informacje:

a) liczbę przedłożonych sporów;

b) zbiorcze podsumowanie wyników tych sporów;

c) średni czas rozstrzygania sporów;

d) najczęstsze powody prowadzące do sporów między stronami.

7b. Aby ułatwić wymianę informacji i najlepszych praktyk, publiczny organ rozstrzygania sporów może zdecydować o dodaniu do sprawozdania zaleceń dotyczących metod unikania lub rozwiązywania takich problemów.

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 ***i szyfrowanie***, aby zapobiec nieuprawnionemu ***ujawnieniu danych i*** dostępowi do danych***, w tym metadanych,*** i zapewnić zgodność z art. ***4,*** 5, 6, ***8,*** 9 i 10, a także z uzgodnionymi postanowieniami umownymi dotyczącymi udostępniania danych. Takie techniczne środki ochrony nie mogą ***nierówno traktować odbiorców danych ani ograniczać prawa*** użytkownika do skutecznego ***uzyskania kopii danych, odzyskania bądź wykorzystania danych, dostępu do danych lub*** dostarczania danych osobom trzecim na podstawie art. 5 ani jakiegokolwiek prawa osoby trzeciej wynikającego z prawa Unii lub przepisów krajowych wdrażających prawo Unii, o których mowa w art. 8 ust. 1. ***W przypadku gdy użytkownik lub posiadacz danych przedstawi osobie trzeciej konkretne istotne dowody na bezprawne wykorzystanie lub nieuprawnione ujawnienie przez odbiorcę danych, na żądanie użytkownika lub posiadacza danych odbiorca danych przekazuje informacje o tym, w jaki sposób dane zostały wykorzystane lub komu zostały udostępnione.***

2. ***W przypadku gdy*** odbiorca danych, który w celu uzyskania danych przekazał posiadaczowi danych ▌ 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***, w tym do stworzenia konkurencyjnego produktu w rozumieniu art. 6 ust. 2 lit. e),*** lub ***bezprawnie*** ujawnił ▌ dane innej osobie ▌, ***odpowiada on za szkody wyrządzone stronie, która ucierpiała na niewłaściwym wykorzystaniu lub ujawnieniu tych danych, i – na żądanie posiadacza danych lub posiadacza tajemnicy przedsiębiorstwa, jeżeli nie są one tą samą osobą prawną*** – musi bez zbędnej zwłoki:

a) ***wykasować udostępnione*** dane ▌ 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.

ba) poinformować użytkownika o nieuprawnionym wykorzystaniu lub ujawnieniu danych oraz o środkach zastosowanych, by położyć kres nieuprawnionemu wykorzystywaniu lub ujawnianiu danych;

bb) powiadomić posiadacza danych o ujawnieniu takich danych.

2a. Jeżeli odbiorca danych naruszy art. 6 ust. 2 lit. a) i b), użytkownikowi przysługują te same prerogatywy co posiadaczowi danych, a odbiorca danych ma takie same obowiązki, jak określono w ust. 2 niniejszego artykułu.

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, ***są nieważne***.

2a. Wszelkie postanowienia umowne zawarte w umowie o udostępnianiu danych między posiadaczami danych a odbiorcami danych, podważające – ze szkodą dla osoby, której dane dotyczą – stosowanie jej praw do ochrony prywatności i danych osobowych, stanowiące odstępstwo od niego lub zmieniające jego skutki, są nieważne.

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 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 ***inne*** przedsiębiorstwo , nie jest wiążące dla tego innego przedsiębiorstwa, ***odbiorcy danych lub użytkownika danych,*** jeżeli postanowienie to jest nieuczciwe.

1a. Postanowienia umownego nie uznaje się za nieuczciwe, jeżeli wynika ono z mającego zastosowanie prawa Unii.

2. Postanowienie umowne jest nieuczciwe, jeżeli cechuje się tym, że ***obiektywnie ogranicza zdolność strony, na którą jednostronnie nałożono to postanowienie, do ochrony jej uzasadnionych interesów handlowych w odniesieniu do przedmiotowych danych lub*** 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***, lub też powoduje znaczny brak równowagi między prawami i obowiązkami stron umowy***.

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***, w tym gdy takie dane zawierają szczególnie chronione dane handlowe lub są chronione tajemnicą przedsiębiorstwa lub prawem własności intelektualnej, bez wcześniejszej zgody właściwych stron***;

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;

ca) narzucenie jednostronnego wyboru właściwej jurysdykcji lub zapłaty kosztów związanych z procedurą;

cb) uniemożliwienie stronie, na którą jednostronnie nałożono to postanowienie, rozwiązania umowy w rozsądnym terminie;

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, istotnej zmiany ustalonej z góry ceny płatnej na podstawie umowy lub jakiegokolwiek innego istotnego warunku dotyczącego udostępnianych danych, bez prawa drugiej strony do rozwiązania umowy, lub*** 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.

6a. Strona, która zaproponowała sporne postanowienie, nie może twierdzić, że jest to postanowienie nieuczciwe.

7. Niniejszy artykuł nie ma zastosowania do postanowień umownych określających główny przedmiot umowy ***i nie ma wpływu na zdolność stron do negocjacji ceny*** do zapłaty.

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

8a. Niniejszy artykuł stosuje się do wszystkich nowych umów zawartych po … [data wejścia w życie niniejszego rozporządzenia]. Przedsiębiorstwom daje się trzy lata po tej dacie na dokonanie przeglądu istniejących zobowiązań umownych, które podlegają niniejszemu rozporządzeniu.

8b. Z uwagi na szybkie tempo pojawiania się innowacji na rynkach Komisja będzie poddawać regularnemu przeglądowi wykaz nieuczciwych postanowień umownych, o których mowa w art. 13, i w razie potrzeby dostosowywać go do nowych praktyk biznesowych.

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. ***Na specjalny*** wniosek***, który jest należycie uzasadniony i dotyczy określonego czasu i zakresu,*** posiadacz danych ***będący osobą prawną*** udostępnia ***dane nieosobowe dostępne w momencie złożenia wniosku, w tym metadane,*** 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.

2a. Niniejszy rozdział nie wyklucza dobrowolnych uzgodnień między przedsiębiorstwami a organami sektora publicznego i instytucjami, agencjami lub organami Unii w zakresie wymiany danych do celów świadczenia usług publicznych, w tym w przypadku wyjątkowej potrzeby, jeżeli przewidują to ich umowy.

Artykuł 15

Wyjątkowa potrzeba skorzystania z danych

Wyjątkowa potrzeba skorzystania z danych ***nieosobowych*** w rozumieniu niniejszego rozdziału ***jest ograniczona w czasie i zakresie*** i uznaje się, że istnieje ▌ w następujących okolicznościach:

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

b) ***w sytuacjach, które nie są sytuacjami kryzysowymi, gdy organ sektora publicznego lub instytucja, agencja lub organ Unii działają na podstawie prawa Unii lub prawa krajowego i zidentyfikowały określone dane, które są im niedostępne, a które są absolutnie niezbędne do realizacji konkretnego zadania leżącego w interesie publicznym i wyraźnie wskazanego w prawie, takiego jak prewencja lub przywracanie*** stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego***, i których organ sektora publicznego lub instytucja, agencja lub organ Unii nie mogły uzyskać w żaden z następujących sposobów: dobrowolne porozumienie; zakup danych na rynku lub poleganie na istniejących obowiązkach udostępnienia danych.***

▌

Artykuł 15a

Pojedynczy punkt do rozpatrywania wniosków organów sektora publicznego

1. Koordynator danych wyznaczony zgodnie z art. 31 jest odpowiedzialny za koordynację wniosków składanych na podstawie art. 14 ust. 1 przez organy sektorowe danego państwa członkowskiego w celu zadbania o to, aby wnioski te spełniały wymóg określony w niniejszym rozdziale, i przekazuje je posiadaczowi danych. Dba on o to, by różne organy sektora publicznego na jego terytorium nie kierowały wielu wniosków do tego samego posiadacza danych.

2. Państwa członkowskie regularnie informują Komisję o wnioskach składanych na podstawie art. 14 ust. 1.

3. W przypadku gdy organy sektora publicznego lub instytucje, agencje lub organy Unii wymagają danych od tego samego posiadacza danych w więcej niż jednym państwie członkowskim ze względu na wyjątkową potrzebę zgodnie z art. 14 ust. 1, właściwe organy państw członkowskich współpracują zgodnie z art. 22 w celu skoordynowania ich wniosków, jeżeli jest to konieczne do zminimalizowania obciążenia administracyjnego spoczywającego na posiadaczach danych.

4. Komisja opracuje wzór wniosku na podstawie art. 17.

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. ▌ Niniejszy rozdział nie ***ma zastosowania do organów*** sektora publicznego ani ***instytucji, agencji i organów*** Unii***, które prowadzą działania*** w zakresie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych lub wykonywania kar, ani do 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.

2a. Przedsiębiorstwa objęte zakresem niniejszego rozdziału informują swoich użytkowników o możliwości udostępniania danych w przypadku wyjątkowych okoliczności.

Artykuł 17

Wnioski o udostępnienie danych

1. ***We wniosku*** o udostępnienie danych na podstawie art. 14 ust. 1 organ sektora publicznego lub instytucja, agencja lub organ Unii musi:

a) ***wystąpić z wnioskiem o dane wchodzące w zakres ich kompetencji i określić, o jakie zbiory danych chodzi***;

b) wykazać wyjątkową potrzebę, z powodu której wnioskuje się o udostępnienie danych***, oraz zgodność z warunkami, o których mowa w art. 15***;

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

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

cb) uzasadnić wybór posiadacza danych, do którego skierowany jest wniosek;

cc) wymienić inne organy sektora publicznego, instytucje, agencje lub organy Unii oraz osoby trzecie, którym żądane dane mają zostać udostępnione;

cd) ujawnić w stosownych przypadkach tożsamość osoby trzeciej, o której mowa w ust. 4 niniejszego artykułu i w art. 21 niniejszego rozporządzenia;

ce) zastosować wszystkie odpowiednie środki bezpieczeństwa ICT związane z przekazywaniem i przechowywaniem danych;

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

da) określić granice geograficzne mające zastosowanie do wniosku o udostępnienie danych;

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

ea) złożyć oświadczenie o zgodnym z prawem i bezpiecznym przetwarzaniu danych, których dotyczy wniosek, w tym o zachowaniu poufności tajemnic przedsiębiorstwa;

eb) zadbać o to, aby udostępnienie danych nie stawiało posiadacza danych w sytuacji, która naruszałaby prawo Unii lub prawo krajowe, ani nie nakładało na posiadacza danych odpowiedzialności za jakiekolwiek naruszenie lub szkody wynikające z dostępu do danych, o które wystąpił organ sektora publicznego, instytucja, agencja lub organ Unii.

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

a) być ***złożony na piśmie i*** sformułowany jasnym, zwięzłym i prostym językiem zrozumiałym dla posiadacza danych;

aa) zostać przedłożony za pośrednictwem właściwego organu;

ab) zawierać szczegóły dotyczące rodzaju danych, których dotyczy wniosek, i odnosić się do danych, które posiadacz danych przechowuje w momencie składania wniosku;

b) być ***uzasadniony i*** 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; ***w stosownych przypadkach określać środki, które należy podjąć zgodnie z art. 19 ust. 2, by zachować poufność tajemnic przedsiębiorstwa, w tym w stosownych przypadkach przez zastosowanie modelowych postanowień umownych, standardów technicznych lub kodeksów postępowania***;

d) dotyczyć ***tylko*** danych nieosobowych;

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

f) ***zostać przekazany koordynatorowi danych, o którym mowa w art. 31, który podaje wniosek*** do wiadomości publicznej w internecie bez zbędnej zwłoki; ***koordynator danych może poinformować organ sektora publicznego lub instytucję, agencję lub organ Unii, jeżeli posiadacz danych przekazał już żądane dane w odpowiedzi na wniosek złożony wcześniej w tym samym celu przez inny organ sektora publicznego lub instytucję, agencję lub organ Unii.***

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 ***oraz rozporządzenia (UE) 2022/868***. Dyrektywa (UE) 2019/1024 ***i rozporządzenie (UE) 2022/868*** nie ***mają*** 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***, wymienionych we wniosku zgodnie z ust. 1 lit. cc),*** w celu realizacji 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. ***Zobowiązuje on umownie osobę trzecią do niewykorzystywania danych do innych celów oraz do nieudostępniania ich innym osobom trzecim. W przypadku gdy organ sektora publicznego lub instytucja, agencja lub organ Unii przekazują lub udostępniają dane na podstawie niniejszego ustępu, bez zbędnej zwłoki powiadamiają o tym posiadacza danych, od którego otrzymały dane. W ciągu pięciu dni roboczych od tego powiadomienia posiadacz danych ma prawo wyrazić uzasadniony sprzeciw wobec przekazania lub udostępnienia danych. W przypadku odrzucenia uzasadnionego sprzeciwu przez organ sektora publicznego bądź instytucję, agencję lub organ Unii posiadacz danych może skierować sprawę do koordynatora danych, o którym mowa w art. 31.*** Organy sektora publicznego, instytucje, agencje lub organy Unii ***oraz osoby trzecie otrzymujące dane muszą wypełniać obowiązki określone w*** art. 19 ▌.

Dane uzyskane zgodnie z niniejszym rozdziałem wykorzystuje się wyłącznie do celów określonych we wniosku. Organy sektora publicznego, instytucje, agencje lub organy Unii zobowiązują umownie osoby trzecie, którym zgodziły się udostępnić dane zgodnie z ust. 4, do niewykorzystywania danych do żadnych innych celów i do nieudostępniania ich innym osobom.

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***, uwzględniając niezbędny czas oraz niezbędne środki techniczne, organizacyjne i prawne***.

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 ***pięciu*** dni roboczych od otrzymania wniosku o udostępnienie danych niezbędnych do zareagowania na niebezpieczeństwo publiczne oraz w ciągu ***30*** dni roboczych w innych przypadkach występowania wyjątkowej potrzeby, powołując się na jeden z następujących powodów:

a) dane są niedostępne ***dla posiadacza danych w momencie składania wniosku;***

aa) stosowane środki bezpieczeństwa dotyczące przekazywania, przechowywania i zachowania poufności są niewystarczające;

ab) podobny wniosek w tym samym celu złożył wcześniej inny organ sektora publicznego albo instytucja, agencja lub organ Unii, a posiadacza danych nie powiadomiono o usunięciu danych zgodnie z art. 19 ust. 1 lit. c);

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

▌

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 ▌ ***pseudonimizuje dane osobowe, które mają zostać udostępnione***.

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 ***koordynatora danych***, o którym mowa w art. 31***, nie naruszając prawa do wniesienia sprawy do sądu cywilnego lub administracyjnego, zgodnie z prawem unijnym lub krajowym***.

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, ***i organizacje statystyczne lub badawcze otrzymujące dane na podstawie wniosku złożonego zgodnie z art. 21 ust. 1***:

▌

b) muszą wdrożyć – o ile konieczne jest przetwarzanie danych osobowych – środki techniczne i organizacyjne chroniące prawa i wolności osób, których dane dotyczą***, oraz zagwarantować wysoki poziom ochrony i zapobiegać nieuprawnionemu ujawnieniu danych***;

ba) muszą wdrożyć niezbędne środki techniczne i organizacyjne w celu zarządzania cyberzagrożeniem, które mogłoby mieć wpływ na poufność, integralność lub dostępność żądanych danych;

bb) muszą powiadomić posiadacza danych, od którego otrzymali dane, o każdym cyberincydencie mającym wpływ na poufność, integralność lub dostępność otrzymanych danych jak najszybciej, ale nie później niż 72 godziny po ustaleniu, że incydent miał miejsce, bez uszczerbku dla obowiązków sprawozdawczych wynikających z rozporządzenia (UE) XXX/XXXX (EUIBAL) i dyrektywy (UE) 2022/2555. Podmioty te ponoszą odpowiedzialność za szkody spowodowane naruszeniem cyberbezpieczeństwa, jeżeli nie wprowadzą uprzednio w życie środków zgodnie z ust. 1 lit. ba).

c) muszą ***usunąć*** dane, gdy tylko przestaną one być niezbędne do określonego celu, i ***bez zbędnej zwłoki*** poinformować posiadacza danych o ich ***usunięciu***.

1a. Organ sektora publicznego, instytucja, agencja lub organ Unii bądź osoba trzecia otrzymujące dane zgodnie z przepisami niniejszego rozdziału nie mogą:

a) wykorzystywać danych do opracowania produktu lub usługi bądź do udoskonalenia istniejącego produktu lub usługi, które konkurują z produktem lub usługą, z których pochodzą te dane;

b) pozyskiwać informacji na temat sytuacji ekonomicznej, aktywów oraz metod produkcji lub działalności posiadacza danych, ani udostępniać danych w tym celu innej osobie trzeciej; lub

c) udostępniać danych innej osobie trzeciej w jakimkolwiek z tych celów.

2. Ujawnienie 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 ***złożonego na podstawie art. 15***. W takim przypadku ***posiadacz danych wskazuje dane chronione jako tajemnice przedsiębiorstwa***. ***Organ*** sektora publicznego lub instytucja, agencja lub organ Unii stosują ***z wyprzedzeniem wszelkie*** odpowiednie środki ***techniczne i organizacyjne uzgodnione z posiadaczem danych lub posiadaczem tajemnicy przedsiębiorstwa, jeśli nie jest to jednocześnie ta sama osoba prawna, niezbędne***, aby zachować poufność tych tajemnic przedsiębiorstwa***, w tym w stosownych przypadkach przez zastosowanie modelowych postanowień umownych, standardów technicznych i kodeksów postępowania***.

2a. Jeżeli organ sektora publicznego lub instytucja, agencja lub organ Unii przekazują lub udostępniają dane osobom trzecim w celu wykonania zadań zleconych im w wyniku eksternalizacji kontroli technicznych lub innych funkcji zgodnie z art. 17 ust. 4, tajemnice przedsiębiorstwa wskazane przez posiadacza danych ujawnia się wyłącznie w zakresie, w jakim są absolutnie niezbędne osobie trzeciej do wykonania zleconych zadań, i pod warunkiem zastosowania z wyprzedzeniem wszystkich szczególnych niezbędnych środków uzgodnionych między posiadaczem danych a tą osobą trzecią, w tym środków technicznych i organizacyjnych służących zachowaniu poufności tych tajemnic przedsiębiorstwa, co obejmuje w stosownych przypadkach zastosowanie modelowych postanowień umownych, standardów technicznych i kodeksów postępowania.

2b. Jeżeli organ sektora publicznego lub instytucja, agencja bądź organ Unii, które złożyły wniosek o udostępnienie danych, lub osoba trzecia, której udostępniono dane zgodnie z art. 17 ust. 4, nie stosują tych środków lub naruszają poufność tajemnic przedsiębiorstwa, posiadacz danych może zawiesić udostępnianie danych wskazanych jako tajemnice przedsiębiorstwa. W takich przypadkach posiadacz danych niezwłocznie powiadamia koordynatora danych państwa członkowskiego, w którym ma siedzibę, zgodnie z art. 31, że zawiesił udostępnianie danych, i wskazuje, których środków nie zastosowano lub które tajemnice przedsiębiorstwa naruszono. Jeżeli organ sektora publicznego lub instytucja, agencja bądź organ Unii lub osoba trzecia chcą zaskarżyć decyzję posiadacza danych o zawieszeniu udostępniania danych, koordynator danych decyduje w rozsądnym terminie, czy dane mają być ponownie udostępniane, a jeżeli tak, to na jakich warunkach.

2c. Organ sektora publicznego lub instytucja, agencja bądź organ Unii odpowiadają za bezpieczeństwo danych, które otrzymują.

2d. Organ sektora publicznego lub instytucja, agencja bądź organ Unii powiadamiają jak najszybciej posiadacza danych w przypadku naruszenia bezpieczeństwa, ale nie później niż w ciągu 48 godzin.

Artykuł 20

Wynagrodzenie w przypadkach wyjątkowej potrzeby

1. ***O ile w prawie unijnym lub krajowym nie określono inaczej, dane*** udostępniane w celu zareagowania na niebezpieczeństwo publiczne na podstawie art. 15 lit. a) są udostępniane nieodpłatnie. ***Organ sektora publicznego lub instytucja, agencja bądź organ Unii, które otrzymały dane, zapewniają publiczne uznanie posiadaczowi danych, jeżeli posiadacz danych zwrócił się do nich o to.***

2. ***Posiadaczowi danych należy się rozsądne wynagrodzenie*** za udostępnienie danych zgodnie z wnioskiem złożonym na podstawie art. 15 ***lit. b)***, a wynagrodzenie takie ***pokrywa co najmniej koszty techniczne i organizacyjne poniesione*** w celu zastosowania się do wniosku, w tym, w stosownych przypadkach, koszty anonimizacji i dostosowania technicznego, powiększone 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.

2a. W przypadku gdy organ sektora publicznego lub instytucja, agencja bądź organ Unii chcą zakwestionować poziom wynagrodzenia zażądany przez posiadacza danych, sprawę należy skierować do koordynatora danych, o którym mowa w art. 31, państwa członkowskiego, w którym posiadacz danych ma siedzibę.

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 ***niezbędnych do osiągnięcia celu***, w którym wystąpiono o dane, lub krajowym urzędom statystycznym***, członkom Europejskiego Systemu Banków Centralnych*** i Eurostatowi do celów tworzenia statystyki publicznej.

2. Osoby fizyczne lub organizacje otrzymujące dane na podstawie ust. 1 muszą prowadzić działalność ***wyłącznie*** 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 ***znaczącym*** 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 bądź instytucja, agencja lub organ Unii ***zamierzają przekazać lub udostępnić*** dane na podstawie ust. 1, powiadamiają o tym posiadacza danych, od którego otrzymano dane. ***To powiadomienie musi zawierać dane identyfikacyjne i kontaktowe osób fizycznych lub organizacji otrzymujących dane, cel przekazania lub udostępnienia danych oraz okres, przez jaki dane te będą wykorzystywane przez podmiot otrzymujący dane. W ciągu pięciu dni roboczych od otrzymania powiadomienia, o którym mowa w akapicie pierwszym, posiadacz danych ma prawo wyrazić uzasadniony sprzeciw wobec przekazania lub udostępnienia danych. W razie odrzucenia sprzeciwu przez organ sektora publicznego bądź instytucję, agencję lub organ Unii posiadacz danych może skierować uzasadniony sprzeciw do koordynatora danych, o którym mowa w art. 31.***

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 ***koordynatora danych*** tego państwa członkowskiego, o którym to ***koordynatorze*** mowa w art. 31. Wymóg ten ma również zastosowanie do wniosków składanych przez instytucje, agencje i organy Unii. ***Właściwy organ państwa członkowskiego, w którym posiadacz danych ma siedzibę, ocenia wniosek.***

4. Po otrzymaniu powiadomienia zgodnie z ust. 3 ***koordynator danych*** 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 ***koordynatora danych***.

ROZDZIAŁ VI

PRZEJŚCIE NA INNE USŁUGI PRZETWARZANIA DANYCH

Artykuł 22a

Definicje

Do celów niniejszego rozdziału stosuje się następujące definicje:

1. ***„usługa przetwarzania danych" oznacza świadczoną na rzecz klienta usługę cyfrową umożliwiającą wszechobecny dostęp na żądanie do wspólnego zbioru konfigurowalnych, skalowalnych i elastycznych zasobów obliczeniowych o charakterze scentralizowanym, rozproszonym lub wysoce rozproszonym, które mogą być szybko zrealizowane i udostępnione przy minimalnym wysiłku pod względem zarządzania lub interakcji z dostawcą usług;***

2. ***„infrastruktura lokalna" oznacza infrastrukturę ICT i zasoby obliczeniowe będące przedmiotem najmu przez klienta lub jego własnością, znajdujące się w jego własnym centrum danych i obsługiwane przez tego klienta lub osobę trzecią;***

3. ***„równoważna usługa" oznacza zestaw usług przetwarzania danych, które mają ten sam główny cel i opierają się na tym samym modelu usługi przetwarzania danych;***

4. ***„możliwość przenoszenia danych z usług przetwarzania danych" oznacza możliwość przeniesienia usługi w chmurze i dostosowania objętych nią danych eksportowalnych między usługami przetwarzania danych klienta, w tym w różnych modelach rozmieszczenia;***

5. ***„zmiana dostawcy" oznacza proces, w ramach którego klient korzystający z usługi przetwarzania danych przechodzi od korzystania z jednej usługi przetwarzania danych do korzystania z drugiej równoważnej usługi lub innej usługi oferowanej przez innego dostawcę usług przetwarzania danych (w tym poprzez pobranie, przetworzenie i przekazanie danych), w czym uczestniczą dostawca wyjściowych usług przetwarzania danych, klient i dostawca docelowych usług przetwarzania danych;***

6. „dane eksportowalne" oznaczają dane wejściowe i wyjściowe, w tym metadane, wygenerowane bezpośrednio lub pośrednio bądź współwygenerowane w wyniku korzystania przez klienta z usługi przetwarzania danych, z wyłączeniem wszelkich aktywów lub danych dostawcy usług przetwarzania danych lub osób trzecich, objętych prawami własności intelektualnej albo będących tajemnicami przedsiębiorstwa lub informacjami poufnymi;

7. „równoważność funkcjonalna" oznacza możliwość przywrócenia na podstawie danych klienta minimalnego poziomu funkcjonalności w środowisku nowej usługi przetwarzania danych po procesie zmiany dostawcy, gdy docelowa usługa oferuje porównywalny rezultat w reakcji na te same dane wejściowe w stosunku do udostępnianych funkcji zapewnianych klientowi na mocy umowy;

8. „opłaty za odejście" oznaczają opłaty za przekazanie danych pobierane od klientów przez jednego dostawcę usług przetwarzania danych za pobranie ich danych przez sieć z infrastruktury ICT innego dostawcy usług przetwarzania danych.

Artykuł 23

Usuwanie przeszkód w skutecznej zmianie dostawcy usług przetwarzania danych

1. Dostawcy usług przetwarzania danych ***w ramach swoich zasobów*** wprowadzają środki przewidziane w art. 24, ***24a, 24b,*** 25 i 26, aby ***umożliwić*** klientom ***przejście*** na inną usługę przetwarzania danych, obejmującą ***równoważną usługę,*** świadczoną przez innego dostawcę usług ***przetwarzania danych, lub w stosownych przypadkach korzystanie z usług kilku dostawców usług przetwarzania danych jednocześnie***. W szczególności dostawcy usług przetwarzania danych ***nie stawiają przeszkód handlowych, technicznych, umownych i organizacyjnych oraz usuwają przeszkody handlowe, techniczne, umowne i organizacyjne,*** które utrudniają klientom:

a) wypowiedzenie umowy o świadczenie usługi po upływie okresu wypowiedzenia wynoszącego maksymalnie ***60*** dni kalendarzowych***, chyba że klient i dostawca wspólnie i wyraźnie uzgodnili w umowie inny okres wypowiedzenia oraz pod warunkiem że obie strony mogą równoprawnie wpływać na treść tej umowy***.

b) zawarcie nowych umów z innym dostawcą usług przetwarzania danych obejmujących ***równoważną usługę*** ;

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

d) ***uzyskanie*** równoważności funkcjonalnej ***w korzystaniu z nowej*** usługi w środowisku informatycznym innego dostawcy lub innych dostawców usług przetwarzania danych obejmujących ***równoważną*** usługę zgodnie z art. 26.

2. Ust. 1 ma zastosowanie wyłącznie do przeszkód związanych z usługami, umowami lub praktykami handlowymi dostawcy ***wyjściowych*** usług ***przetwarzania danych***.

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 ***lub w stosownych przypadkach przeniesienia do lokalnej infrastruktury ICT*** muszą być jasno określone w pisemnej umowie***, którą udostępnia się klientowi w sposób przyjazny dla użytkownika przed jej podpisaniem***. Nie naruszając przepisów dyrektywy (UE) 2019/770, ***dostawca usług przetwarzania danych dopilnowuje, by w umowie były ujęte*** 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 ***eksportowalnych*** danych, aplikacji i aktywów cyfrowych ***do lokalnej infrastruktury ICT bez zbędnej zwłoki, a w każdym razie nie później niż po upływie*** obowiązkowego maksymalnego okresu przejściowego wynoszącego ***90*** dni kalendarzowych, podczas którego dostawca usług przetwarzania danych:

(i) ***w rozsądnych granicach*** wspomaga proces zmiany dostawcy ***przez cały czas jego trwania i ułatwia ten proces***;

(ii) ***postępuje z należytą starannością w celu utrzymania ciągłości działania i wysokiego poziomu bezpieczeństwa usługi oraz, biorąc pod uwagę przebieg procesu zmiany dostawcy,*** zapewnia ***w jak największym stopniu*** ciągłość świadczenia ***istotnych*** funkcji lub usług ***w ramach zasobów dostawcy wyjściowych usług przetwarzania danych i zgodnie ze zobowiązaniami umownymi***;

(iia) udziela jasnych informacji o znanych zagrożeniach dla ciągłości świadczenia odpowiednich funkcji lub usług po stronie dostawcy wyjściowych usług przetwarzania danych.

aa) wykaz dodatkowych usług do dyspozycji klienta ułatwiających proces zmiany dostawcy, takich jak test procesu zmiany dostawcy;

ab) zobowiązanie dostawcy usług przetwarzania danych do pomocy w opracowaniu strategii odejścia klienta w odniesieniu do usług objętych umową, w tym poprzez dostarczenie wszystkich istotnych informacji;

b) ***szczegółową*** specyfikację wszystkich kategorii danych i aplikacji, które można ***przenieść*** w trakcie procesu zmiany dostawcy, w tym co najmniej wszystkich danych ***eksportowalnych***;

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 ***przetwarzania danych***, zgodnie z ust. 1 lit. a) i ust. 2;

ca) zobowiązanie dostawcy usług przetwarzania danych do usunięcia wszystkich eksportowalnych danych byłego klienta po upływie czasu określonego w ust. 1 lit. c) niniejszego artykułu;

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 ***14*** dni roboczych od złożenia wniosku o zmianę dostawcy, należycie ***uzasadnia*** techniczną niewykonalność i ***wskazuje*** alternatywny okres przejściowy, który nie może przekroczyć ***9*** miesięcy. Zgodnie z ust. 1 niniejszego artykułu ▌ciągłość świadczenia usług musi być zapewniona przez cały alternatywny okres przejściowy, o którym mowa w art. 25 ust. 2. ***Klient zachowuje prawo do przedłużenia w razie potrzeby tego okresu przed rozpoczęciem procesu zmiany dostawcy lub już w jego trakcie.***

Artykuł 24a

Obowiązek informowania spoczywający na dostawcach docelowych usług przetwarzania danych

Dostawca docelowych usług przetwarzania danych przekazuje klientowi informacje na temat istniejących procedur zmiany dostawcy i przejścia na usługę przetwarzania danych, gdy jest ona usługą docelową, w tym informacje o dostępnych metodach i formatach przenoszenia, a także o limitach i ograniczeniach technicznych znanych dostawcy docelowych usług przetwarzania danych.

Artykuł 24b

Obowiązek działania w dobrej wierze

Wszystkie zaangażowane strony, w tym dostawcy docelowych usług przetwarzania danych, współpracują w dobrej wierze, by zadbać o powodzenie procesu zmiany dostawcy, umożliwić terminowe przekazanie niezbędnych danych i utrzymać ciągłość świadczenia usługi.

Artykuł 25

Stopniowe wycofywanie opłat z tytułu zmiany dostawcy

1. Od dnia [***data wejścia w życie niniejszego rozporządzenia***] r. dostawcy usług przetwarzania danych nie nakładają na klientów ***będących konsumentami*** żadnych opłat za proces zmiany dostawcy.

2. Od dnia [data X, data wejścia w życie ***niniejszego rozporządzenia***] r. do dnia [data X + 3 lata] r. dostawcy usług przetwarzania danych mogą nakładać na ***klientów w kontekście relacji między przedsiębiorstwami*** obniżone opłaty za proces zmiany dostawcy***, co zwłaszcza dotyczy opłat za wyjście***.

2a. Od dnia [3 lata od dnia wejścia w życie niniejszego rozporządzenia] r. dostawcy usług przetwarzania danych nie mogą nakładać żadnych opłat w procesie 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 ***oraz muszą mieć związek z obowiązkowymi operacjami, które dostawca usług przetwarzania danych musi wykonać w ramach tego procesu zmiany dostawcy***.

3a. Standardowych opłat abonamentowych lub opłat za usługę oraz opłat za czynności w ramach profesjonalnej usługi przeniesienia, wykonane przez dostawcę usług przetwarzania danych na wniosek klienta o wsparcie procesu zmiany dostawcy, nie uważa się za opłaty za zmianę dostawcy do celów niniejszego artykułu.

3b. Przed zawarciem umowy z klientem dostawca usług przetwarzania danych przekazuje klientowi jasne informacje o opłatach nakładanych na klienta w związku z procesem zmiany dostawcy zgodnie z art. 2 oraz o opłatach, o których mowa w ust. 3a, a także w stosownych przypadkach udziela informacji o usługach związanych z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znaczącej ingerencji w architekturę danych, aplikacji lub usług. W stosownych przypadkach dostawca usług przetwarzania danych podaje te informacje klientom do wiadomości publicznej za pośrednictwem specjalnej sekcji swojej strony internetowej lub w inny łatwo dostępny sposób.

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 ***i obniżenie*** opłat z tytułu zmiany dostawcy opisane w ust. 1 ***i 2*** niniejszego artykułu zostało osiągnięte w terminie określonym w ***tychże ustępach***.

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 ***podjąć rozsądne środki będące w jego mocy, by umożliwić*** klientowi po przejściu na usługę obejmującą ten sam rodzaj usługi oferowaną przez innego dostawcę usług przetwarzania danych ***osiągnięcie równoważności funkcjonalnej*** w korzystaniu z nowej usługi***, chyba że taką równoważność funkcjonalną zapewnia dostawca docelowych usług przetwarzania danych. Dostawca wyjściowych usług przetwarzania danych ułatwia ten proces, zapewniając zasoby, odpowiednie informacje, dokumentację, wsparcie techniczne oraz, w stosownych przypadkach, niezbędne narzędzia.***

2. ▌***Dostawcy*** usług przetwarzania danych***, w tym dostawcy docelowych usług przetwarzania danych,*** muszą udostępniać otwarte interfejsy publicznie i nieodpłatnie***, aby ułatwić zmianę dostawcy tych usług, możliwość przenoszenia danych i interoperacyjność. Zgodnie z ust. 1 niniejszego artykułu usługi te umożliwiają również to, by określona usługa, o ile nie ma poważnych przeszkód, mogła zostać wyodrębniona z umowy i udostępniona na potrzeby zmiany dostawcy w sposób interoperacyjny.***

3. ▌Dostawcy usług przetwarzania danych muszą zapewniać zgodność z otwartymi specyfikacjami w zakresie interoperacyjności ***i możliwości przenoszenia*** lub normami europejskimi w zakresie interoperacyjności określonymi zgodnie z art. 29 ust. 5 ▌.

3a. Dostawcy usług przetwarzania danych, w odniesieniu do których w repozytorium, o którym mowa w art. 29 ust. 5, opublikowano nową otwartą specyfikację lub nową normę europejską w zakresie interoperacyjności i możliwości przenoszenia, mają prawo do rocznego okresu przejściowego, by wywiązać się z obowiązku, o którym mowa w ust. 3 niniejszego artykułu.

4. Jeżeli w przypadku ▌***danej równoważnej*** usługi nie istnieją otwarte specyfikacje lub normy europejskie w zakresie interoperacyjności ***i możliwości przenoszenia***, o których mowa w ust. 3 ***niniejszego artykułu***, dostawca usług przetwarzania danych na wniosek klienta eksportuje***, jeżeli jest to technicznie wykonalne,*** wszystkie dane ***eksportowalne*** w uporządkowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego***, o którym poinformowano klienta zgodnie ze strategią odejścia, o której mowa w art. 24 ust. 1 lit. ab), chyba że klient zgodzi się na inny format***.

4a. Od dostawców usług przetwarzania danych nie można wymagać opracowania nowych technologii lub usług, ujawnienia lub przekazania zastrzeżonych lub poufnych danych lub technologii klientowi lub innemu dostawcy usług przetwarzania danych ani stworzenia zagrożenia dla bezpieczeństwa i integralności usług klienta lub dostawcy.

Artykuł 26a

Zwolnienia dotyczące niektórych usług przetwarzania danych

1. Obowiązki określone w art. 23 ust. 1 lit. d) oraz w art. 25 i 26 nie mają zastosowania do usług przetwarzania danych, które zostały stworzone na zamówienie.

2. Obowiązki określone w niniejszym rozdziale nie mają zastosowania do usług przetwarzania danych świadczonych bezpłatnie, które funkcjonują na zasadzie próbnej lub służą wyłącznie testowaniu i ocenie ofert produktów biznesowych.

Artykuł 26b

Rozstrzyganie sporów

1. Klienci mają dostęp do organów rozstrzygania sporów, certyfikowanych zgodnie z art. 10 ust. 2, by rozstrzygały spory dotyczące naruszeń praw klientów i niewywiązania się z obowiązków przez dostawców usług przetwarzania danych w kontekście zmiany dostawcy takich usług. Klient ma prawo zezwolić osobie trzeciej na dochodzenie roszczeń prawnych w jego imieniu.

2. Art. 10 ust. 3–9 ma zastosowanie do rozstrzygania sporów między klientami a dostawcami usług przetwarzania danych w związku ze zmianą dostawcy takich usług.

ROZDZIAŁ VII

ZABEZPIECZENIA DANYCH NIEOSOBOWYCH W KONTEKŚCIE MIĘDZYNARODOWYM

Artykuł 27

Dostęp międzynarodowy i przekazywanie międzynarodowe

1. Dostawcy usług przetwarzania danych wprowadzają wszelkie ▌środki techniczne, prawne i organizacyjne, w tym ustalenia umowne, w celu zapobiegania międzynarodowemu przekazywaniu danych nieosobowych przechowywanych w Unii lub dostępowi władz ***państwa trzeciego*** do tych danych, w przypadku gdy takie przekazywanie lub dostęp ***naruszałyby prawo*** Unii lub ***prawo*** odpowiedniego państwa członkowskiego, bez uszczerbku dla 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 ***zostają*** uznane lub ***są*** 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 ***po przeprowadzeniu kontroli przez właściwe organy lub władze, na podstawie niniejszego rozporządzenia, mającej na celu ocenę, czy, oprócz zgodności z przepisami właściwego prawa unijnego lub krajowego, spełnione zostały następujące warunki***:

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 ***Komisji, koordynatora danych***, zgodnie z niniejszym rozporządzeniem, ***bądź do właściwych organów lub władz*** w celu ustalenia, czy warunki te zostały spełnione, w szczególności jeżeli uzna, że decyzja może dotyczyć ***tajemnic przedsiębiorstwa i innych*** szczególnie chronionych danych handlowych ***oraz treści chronionych prawem własności intelektualnej*** lub naruszać interesy bezpieczeństwa narodowego lub obrony Unii lub jej państw członkowskich. ***Jeżeli adresat nie otrzyma odpowiedzi w ciągu miesiąca lub jeżeli w opinii właściwe organy stwierdzą, że nie spełniono warunków, adresat odrzuca na tej podstawie wniosek o przekazanie danych lub dostęp do nich.***

Europejska Rada ds. Innowacji w zakresie Danych – ustanowiona rozporządzeniem ***(UE) 2022/868 i o której mowa w art. 31a niniejszego rozporządzenia*** – 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 ***przez odpowiedni właściwy podmiot lub organ***.

4a. W przypadku gdy dostawca usług przetwarzania danych ma powody, by sądzić, że przekazanie danych nieosobowych lub dostęp do nich może prowadzić do ryzyka ponownej identyfikacji danych nieosobowych lub zanonimizowanych, przed przekazaniem danych lub udzieleniem do nich dostępu dostawca zwraca się o zezwolenie do odpowiednich organów lub organów właściwych zgodnie z mającym zastosowanie prawem o ochronie danych.

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 przestrzeni danych

1. ***Uczestnicy przestrzeni danych, którzy oferują oparte na danych usługi innym uczestnikom,*** 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 ***w formacie nadającym się do odczytu maszynowego***, 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***, jeśli jest to techniczne wykonalne i nie utrudnia prawidłowego funkcjonowania produktu***;

d) muszą być zapewnione środki umożliwiające interoperacyjność ▌ umów ***o udostępnianie danych*** w ramach usług i działań.

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***, po konsultacji z Europejską Radą ds. Innowacji w zakresie Danych zgodnie z art. 29 i art. 30 lit. f) i h) rozporządzenia (UE) 2022/868 oraz zgodnie z art. 38 niniejszego rozporządzenia,*** w celu uzupełnienia niniejszego rozporządzenia poprzez sprecyzowanie zasadniczych wymagań, o których mowa w ust. 1 ***niniejszego artykułu***.

3. ***Uczestnicy przestrzeni danych, którzy oferują dane lub oparte na danych usługi innym uczestnikom*** 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 ▌, w zakresie, w jakim wspomniane normy obejmują te wymagania.

3a. Uczestnicy w określonej przestrzeni danych uzgadniają zasady, na podstawie których definiują między sobą zakresy odpowiedzialności dotyczące tych wymogów.

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***, opracowanych w sposób otwarty, przejrzysty, neutralny pod względem technologicznym, branżowy i inkluzywny, zgodnie z rozdziałem II rozporządzenia (UE) nr 1025/2012 i z uwzględnieniem – w stosownych przypadkach – już istniejących standardów, dobrych praktyk, norm, specyfikacji technicznych i odpowiednich norm otwartego oprogramowania, a także potrzeb MŚP***.

5. Komisja ***może przyjąć*** – 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***. Przed przyjęciem tych aktów wykonawczych Komisja zasięga porady Europejskiej Rady ds. Innowacji w zakresie Danych i uwzględnia jej odpowiednie stanowiska, o których mowa w art. 30 lit. f) rozporządzenia (UE) 2022/868, i przyjmuje je*** zgodnie z procedurą sprawdzającą, o której mowa w art. 39 ust. 2.

6. Komisja może przyjąć wytyczne ***zaproponowane przez Europejską Radę ds. Innowacji w zakresie Danych zgodnie z art. 30 lit. h) rozporządzenia (UE) 2022/868*** 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 ***i możliwość przenoszenia*** usług przetwarzania danych

1. Otwarte specyfikacje w zakresie interoperacyjności i ***możliwości przenoszenia oraz*** normy europejskie w zakresie interoperacyjności ***i możliwości przenoszenia*** usług przetwarzania danych:

a) ***jeżeli jest to technicznie wykonalne,*** są ukierunkowane na osiągnięcie interoperacyjności ***i możliwości przenoszenia*** między różnymi usługami przetwarzania danych, które obejmują ***równoważne usługi***;

b) zwiększają możliwość przenoszenia aktywów cyfrowych między różnymi usługami przetwarzania danych, które obejmują ***równoważne usługi***;

c) ***ułatwiają***, jeżeli jest to technicznie wykonalne, równoważność funkcjonalną różnych usług przetwarzania danych ***określonych w art. 1 ust. 26***, które obejmują ***równoważne usługi;***

ca) nie mogą mieć negatywnego wpływu na bezpieczeństwo i integralność usług i danych;

cb) są opracowane w sposób umożliwiający postęp techniczny oraz wprowadzanie nowych funkcji i innowacje w usługach przetwarzania danych.

2. Otwarte specyfikacje w zakresie interoperacyjności i ***możliwości przenoszenia oraz*** normy europejskie w zakresie interoperacyjności ***i możliwości przenoszenia*** 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 ***i możliwości przenoszenia*** muszą być zgodne z pkt 3 i 4 załącznika II do rozporządzenia (UE) nr 1025/2012.

3a. Otwarte specyfikacje dotyczące interoperacyjności i możliwości przenoszenia oraz normy europejskie nie mogą zakłócać rynku usług przetwarzania danych ani ograniczać rozwoju wszelkich nowych konkurencyjnych i innowacyjnych technologii lub rozwiązań ani wszelkich technologii lub rozwiązań, które będą na nich oparte.

4. ***Po uwzględnieniu odpowiednich międzynarodowych i europejskich norm i inicjatyw samoregulujących*** 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 ***równoważnych*** usług przetwarzania danych. ***W standaryzacji uwzględnia się potrzeby MŚP.***

5. Do celów art. 26 ust. 3 niniejszego rozporządzenia Komisja – ***po konsultacji z Europejską Radą ds. Innowacji w zakresie Danych zgodnie z art. 29 i art. 30 lit. f) i h) rozporządzenia (UE) 2022/868*** – jest uprawniona do przyjmowania aktów delegowanych ***uzupełniających niniejsze rozporządzenie*** zgodnie z art. 38 ***niniejszego rozporządzenia*** w celu opublikowania odniesienia do otwartych ▌norm w zakresie interoperacyjności ***i możliwości przenoszenia*** usług przetwarzania danych w centralnym repozytorium norm Unii dotyczących interoperacyjności usług przetwarzania danych ***i możliwości przenoszenia*** usług przetwarzania danych ***opracowanych przez właściwe organizacje normalizacyjne lub organizacje, o których mowa w ust. 3 załącznika II do rozporządzenia (UE) nr 1025/2012***, 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

▌***Strona oferująca*** inteligentne umowy ▌w kontekście umowy o udostępnienie danych musi spełniać następujące zasadnicze wymagania:

a) odporność ***i kontrola dostępu***: zapewnienie, aby inteligentna umowa została opracowana w sposób umożliwiający ***rygorystyczne mechanizmy kontroli dostępu i*** 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; ***w związku z tym należy jasno i przejrzyście określić warunki, na jakich inteligentna umowa może zostać zresetowana lub może zostać wydane polecenie, by uległa rozwiązaniu bądź zawieszeniu. W szczególności należy ocenić, na jakich warunkach powinno być dopuszczalne rozwiązanie lub zawieszenie umowy bez zgody drugiej strony;***

ba) równoważność: inteligentna umowa zapewnia ten sam poziom ochrony i pewności prawa co inne umowy wygenerowane odmiennymi środkami;

bb) ochrona poufności tajemnic przedsiębiorstwa: dopilnowanie, aby inteligentną umowę opracowano tak, by zapewniała poufność tajemnic przedsiębiorstwa zgodnie z niniejszym rozporządzeniem.

▌

ROZDZIAŁ IX

WDROŻENIE I EGZEKWOWANIE

Artykuł 31

Koordynator danych

1. Każde państwo członkowskie wyznacza ***niezależny*** właściwy organ ***koordynujący („koordynatora danych") odpowiedzialny*** za stosowanie i wdrażanie niniejszego rozporządzenia***, za koordynację działań powierzonych temu państwu członkowskiemu oraz za pełnienie funkcji pojedynczego punktu kontaktowego dla Komisji, w odniesieniu do wdrażania niniejszego rozporządzenia i reprezentowania państwa członkowskiego w Europejskiej Radzie ds. Innowacji w zakresie Danych, zgodnie z art. 31a***.

1a. 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. Europejski Inspektor Ochrony Danych jest odpowiedzialny za monitorowanie stosowania niniejszego rozporządzenia w zakresie, w jakim dotyczy ono instytucji, organów, urzędów i agencji Unii. W stosownych przypadkach stosuje się odpowiednio art. 62 rozporządzenia (UE) 2018/1725. Zadania i uprawnienia organów nadzorczych są wykonywane w odniesieniu do przetwarzania danych osobowych.

2. Nie naruszając ust. 1 niniejszego artykułu***, koordynatorzy danych zapewniają współpracę między właściwymi organami krajowymi odpowiedzialnymi za monitorowanie innych unijnych lub krajowych aktów prawnych w dziedzinie usług w zakresie danych i łączności elektronicznej, a szczególnie***:

▌

b) w odniesieniu do konkretnych kwestii sektorowych dotyczących ***dostępu do*** danych w związku z wdrażaniem niniejszego rozporządzenia respektuje się kompetencje organów sektorowych ***bez uszczerbku dla przepisów dotyczących konfliktów kompetencji***;

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 ***koordynatora danych*** 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***, podejmowanie dotyczących tych skarg decyzji*** oraz prowadzenie postępowań, w odpowiednim zakresie, w przedmiocie tych skarg, a także ***regularne*** 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 ***skutecznych, proporcjonalnych i*** odstraszających kar pieniężnych, które mogą obejmować kary okresowe i kary z mocą wsteczną, lub wszczynanie postępowania sądowego w celu nałożenia grzywien;

e) monitorowanie rozwoju technologicznego ***i sytuacji gospodarczej mających*** znaczenie dla udostępniania i wykorzystywania danych ***w celu lepszego egzekwowania niniejszego rozporządzenia***;

f) współpracę z ***koordynatorami danych*** innych państw członkowskich w celu zapewnienia spójnego***, szybkiego i skutecznego*** stosowania niniejszego rozporządzenia, w tym wymianę wszystkich istotnych informacji drogą elektroniczną bez zbędnej zwłoki;

fa) współpracę ze wszystkimi odpowiednimi właściwymi organami (zgodnie z innymi przepisami prawa Unii) oraz z Europejską Radą Ochrony Danych Europejskiego i Europejską Radą ds. Innowacji w zakresie Danych, aby dopilnować, by obowiązki wynikające z tego rozporządzenia były egzekwowane spójnie z innymi przepisami prawa Unii;

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, ***koordynator danych*** przy wykonywaniu zadań i uprawnień powierzonych ***mu*** na mocy ust. 3 niniejszego artykułu współpracuje z ***Europejską Radą ds. Innowacji w zakresie Danych oraz***, w stosownych przypadkach, z organem nadzorczym odpowiedzialnym za monitorowanie stosowania rozporządzenia (UE) 2016/679 ***i z Europejskim Inspektorem Ochrony Danych***, aby zapewnić spójne stosowanie niniejszego rozporządzenia. W takich przypadkach odpowiednie państwa członkowskie wyznaczają właściwy organ koordynujący.

5. Państwa członkowskie przekazują Komisji ***i Radzie ds. Innowacji w zakresie Danych*** nazwy ***koordynatorów danych*** 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, ***koordynatorzy danych działają niezależnie i bezstronnie oraz pozostają wolni*** 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 ***wyznaczony koordynator danych dysponował wystarczającymi*** zasobami ***kadrowymi i technicznymi, wiedzą fachową, lokalami i infrastrukturą niezbędnymi do skutecznego działania i odpowiedniego wykonywania*** swoich zadań zgodnie z niniejszym rozporządzeniem.

7a. Podmioty objęte zakresem niniejszego rozporządzenia podlegają jurysdykcji państwa członkowskiego, w którym dany podmiot ma siedzibę.

7b. Użytkownik, posiadacz danych lub odbiorca danych, który jest osobą prawną i nie ma siedziby w Unii, lecz podlega obowiązkom wynikającym z niniejszego rozporządzenia, wyznacza przedstawiciela prawnego w jednym z państw członkowskich, w których mają siedzibę jego odpowiedni kontrahenci.

7c. Właściwe organy na mocy niniejszego rozporządzenia są uprawnione do żądania od użytkowników, posiadaczy danych lub odbiorców danych, którzy są osobami prawnymi, bądź ich przedstawicieli prawnych wszystkich informacji niezbędnych do zweryfikowania zgodności z wymogami niniejszego rozporządzenia. Każdy wniosek o informacje musi być proporcjonalny do wykonywanego zadania i musi być uzasadniony.

7d. W przypadku gdy użytkownik, posiadacz danych lub odbiorca danych, który jest osobą prawną i nie ma siedziby w Unii, nie wyznaczy przedstawiciela prawnego lub przedstawiciel prawny nie przedstawi – na wniosek właściwego organu – niezbędnych informacji, które w pełni wykazują zgodność z niniejszym rozporządzeniem, właściwy organ jest uprawniony do odroczenia rozpoczęcia świadczenia powiązanych usług lub zawieszenia świadczenia powiązanych usług przez posiadaczy danych lub rozpatrywania wniosków o dostęp do danych składanych przez użytkowników lub odbiorców danych, którzy są osobami prawnymi, do czasu wyznaczenia przedstawiciela prawnego lub przekazania niezbędnych informacji.

Artykuł 31a

Wzajemna pomoc

1. Koordynatorzy danych i Komisja ściśle ze sobą współpracują i udzielają sobie wzajemnej pomocy w celu spójnego i skutecznego stosowania niniejszego rozporządzenia. Wzajemna pomoc obejmuje w szczególności wymianę wszystkich informacji zgodnie z niniejszym artykułem drogą elektroniczną oraz obowiązek informowania wszystkich właściwych organów i Komisji przez koordynatora danych zainteresowanego państwa członkowskiego o wszczęciu dochodzenia.

2. Do celów dochodzenia koordynator danych miejsca prowadzenia działalności przez przedsiębiorstwo może zwrócić się do innych koordynatorów danych o dostarczenie konkretnych informacji będących w ich posiadaniu lub o skorzystanie przez nie z uprawnień dochodzeniowych w odniesieniu do konkretnych informacji dostępnych w ich państwie członkowskim. W stosownych przypadkach koordynator danych otrzymujący wniosek może zaangażować w sprawę inne właściwe organy lub inne organy publiczne danego państwa członkowskiego.

3. Koordynator danych otrzymujący wniosek na podstawie ust. 2 stosuje się do takiego wniosku i bez zbędnej zwłoki informuje właściwy organ zainteresowanego państwa członkowskiego o podjętych działaniach.

4. Europejska Rada ds. Innowacji w zakresie Danych powinna wspierać wzajemną wymianę informacji między właściwymi organami, a także doradzać Komisji i pomagać jej we wszystkich kwestiach objętych niniejszym rozporządzeniem, które wchodzą w zakres kompetencji rady zgodnie z art. 30 rozporządzenia (UE) 2022/868. Koordynatorzy danych reprezentują państwa członkowskie w Europejskiej Radzie ds. Innowacji w zakresie Danych utworzonej na mocy rozporządzenia (UE) 2022/868.

Artykuł 32

Prawo do wniesienia skargi do ***koordynatora danych***

1. Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej osoby fizyczne i prawne mają prawo wnieść skargę, indywidualnie lub ▌, zbiorowo, do ***koordynatora danych*** w państwie członkowskim, w którym mają miejsce zwykłego pobytu, miejsce pracy lub siedzibę, jeżeli sądzą, że ich prawa wynikające z niniejszego rozporządzenia zostały naruszone. ***Taka skarga może wynikać z zawieszenia udostępniania danych wskazanych jako tajemnice przedsiębiorstwa po otrzymaniu powiadomienia od posiadacza danych zgodnie z art. 4 ust. 3, art. 5 ust. 8 lub art. 19 ust. 2b.***

2. ***Koordynator danych***, do którego wniesiono skargę, informuje skarżącego ***zgodnie z prawem krajowym*** o przebiegu postępowania i podjętej decyzji.

3. Właściwe organy ***od początku procesu*** współpracują w celu ***skutecznego i terminowego*** rozpatrywania i rozstrzygania skarg, w tym ***poprzez wyznaczanie rozsądnych terminów podejmowania formalnych decyzji, zapewnienie równego traktowania stron, zapewnianie składającym skargę prawa do bycia wysłuchanym i dostępu do akt przez cały czas trwania procedury oraz*** 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 32a

Pełnomocnictwo

1. Bez uszczerbku dla dyrektywy (UE) 2020/1828 lub dla wszelkich innych rodzajów przedstawicielstwa na mocy prawa krajowego użytkownicy, posiadacze danych i odbiorcy danych mają co najmniej prawo umocować podmiot, organizację lub zrzeszenie do wykonania w ich imieniu praw przyznanych niniejszym rozporządzeniem, pod warunkiem że taki podmiot, taka organizacja lub takie zrzeszenie spełniają wszystkie następujące warunki:

a) prowadzą działalność nienastawioną na zysk;

b) zostały należycie ustanowione zgodnie z prawem państwa członkowskiego;

c) ich cele statutowe obejmują uzasadniony interes polegający na zapewnieniu zgodności z niniejszym rozporządzeniem.

Artykuł 32b

Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko właściwemu organowi

1. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każdy użytkownik, posiadacz danych i odbiorca danych ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji właściwego organu dotyczącej tego użytkownika.

2. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każdy użytkownik ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli właściwy organ nie rozpatrzył szybko skargi lub nie poinformował użytkownika, posiadacza danych i odbiorcy danych w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 32.

3. Postępowanie przeciwko właściwemu organowi zostaje wszczęte przed sądem państwa członkowskiego, w którym użytkownik lub reprezentująca go organizacja mają miejsce zwykłego pobytu, miejsce pracy lub siedzibę.

4. Jeżeli postępowanie zostało wszczęte przeciwko decyzji właściwego organu, którą poprzedziła opinia lub decyzja Europejskiej Rady Ochrony Danych w ramach mechanizmu spójności, organ nadzorczy przekazuje sądowi tę opinię lub decyzję.

Artykuł 32c

Prawo do skutecznego środka ochrony prawnej przed sądem

1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym na mocy dyrektywy (UE) 2020/1828, oraz prawa do wniesienia skargi do właściwego organu zgodnie z art. 32b każdy użytkownik, posiadacz danych i odbiorca danych ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna, że prawa przysługujące mu na mocy niniejszego rozporządzenia zostały naruszone w wyniku nieprzestrzegania przepisów niniejszego rozporządzenia.

2. Postępowanie przeciwko posiadaczowi danych, stronie trzeciej lub odbiorcy danych wszczyna się przed sądem państwa członkowskiego, w którym użytkownik ma miejsce zwykłego pobytu, miejsce pracy lub siedzibę.

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.

1a. Państwa członkowskie uwzględniają następujące niewyczerpujące kryteria nakładania kar za naruszenia niniejszego rozporządzenia;

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

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

c) wszelkie wcześniejsze naruszenia dokonane przez stronę naruszającą;

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

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

2. Do dnia [data rozpoczęcia stosowania rozporządzenia] r. państwa członkowskie powiadamiają Komisję***, Europejską Radę Ochrony Danych i Europejską Radę ds. Innowacji w zakresie Danych*** o tych przepisach i środkach, a także powiadamiają ***je*** niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą. ***Komisja prowadzi i regularnie aktualizuje łatwo dostępny publiczny rejestr tych środków.***

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 ***oraz standardowe klauzule umowne na potrzeby umów o przetwarzanie w chmurze, w oparciu o zasady dotyczące zapewniania sprawiedliwych, rozsądnych i niedyskryminujących warunków***, aby pomóc stronom w sporządzaniu i negocjowaniu umów przewidujących zrównoważone prawa i obowiązki wynikające z umowy. ***Takie modelowe postanowienia umowne obejmują co najmniej następujące elementy:***

a) prawo do przedterminowego rozwiązania umowy i warunki rekompensaty w przypadku przedterminowego rozwiązania umowy;

b) politykę zatrzymywania i przechowywania danych;

c) czytelność danych z punktu widzenia użytkownika, w tym informacje na temat metadanych i deszyfrowania;

d) ochronę i zachowanie poufności tajemnic przedsiębiorstwa zgodnie z niniejszym rozporządzeniem.

Modelowe postanowienia umowne, o których mowa w akapicie pierwszym, są publikowane i bezpłatnie udostępniane w łatwo dostępnym formacie elektronicznym.

ROZDZIAŁ X

NIESTOSOWANIE PRAWA SUI GENERIS ***PRZEWIDZIANEGO*** W DYREKTYWIE ***96/9/WE DO BAZ DANYCH ZAWIERAJĄCYCH OKREŚLONE DANE***

Artykuł 35

Bazy danych zawierające określone dane

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 ***objętych zakresem niniejszego rozporządzenia***.

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

1. 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) wykorzystywanie danych przez użytkowników, posiadaczy danych, odbiorców danych i osoby trzecie, rozwój praktyk monetyzacji w europejskiej gospodarce opartej na danych, a także opracowywanie uzgodnień dotyczących udostępniania danych, w tym dynamiki rynkowej w zakresie przestrzeni danych i usług pośrednictwa w zakresie danych;

-aa) wpływ obowiązków technicznych i administracyjnych związanych z przestrzeganiem niniejszego rozporządzenia, w szczególności rozdziału II, na uczestników z branży, również z myślą o zwolnieniach dla MSP;

a) inne kategorie lub rodzaje danych, które mają być udostępniane;

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

ba) stwierdzenie, czy przepisy niniejszego rozporządzenia dotyczące tajemnic przedsiębiorstwa zapewniają poszanowanie tajemnic przedsiębiorstwa bez uszczerbku dla dostępu do danych i wymiany danych; w szczególności ocenia się, czy i jak zapewniono poufność tajemnic przedsiębiorstwa w praktyce mimo ich ujawnienia zarówno w kontekście wymiany danych z osobami trzecimi, jak i w kontekście wymiany między przedsiębiorstwami a organami administracji. Ocenę tę przeprowadza się w ścisłym powiązaniu ze sprawozdaniem z oceny dyrektywy (UE) 2016/943, oczekiwanym do 9 czerwca 2026 r., zgodnie z art. 18 ust. 3 tej dyrektywy.

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;

ea) interakcje między niniejszym rozporządzeniem a innymi odpowiednimi przepisami prawa Unii w celu analizy ewentualnych kolidujących ze sobą regulacji, nadmiernej regulacji lub luk prawnych.

eb) wkład niniejszego rozporządzenia w zapewnienie atrakcyjności ekonomicznej gromadzenia i wykorzystywania wysokiej jakości zbiorów danych przez przedsiębiorstwa unijne;

ec) wkład niniejszego rozporządzenia w innowacje i promowanie rozwoju przedsiębiorstw typu start-up i MŚP wykorzystujących zaawansowane technologie, a także w umożliwianie europejskim użytkownikom dostępu do najnowocześniejszych usług obliczeniowych;

ed) stosowanie i funkcjonowanie art. 27 w sprawie dostępu międzynarodowego do danych i przekazywania międzynarodowego danych.

1a Na podstawie tego sprawozdania Komisja w stosownym przypadku przedkłada Parlamentowi i Radzie wniosek ustawodawczy dotyczący zmiany niniejszego rozporządzenia.

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 ***po upływie 18*** miesięcy od dnia wejścia życie niniejszego rozporządzenia] ▌.

Obowiązki wynikające z art. 4 ust. 1 mają zastosowanie do usług powiązanych wprowadzonych na rynek w ciągu pięciu lat od wejścia w życie niniejszego rozporządzenia i tylko w przypadku, gdy dostawca usługi powiązanej jest w stanie zdalnie wdrożyć mechanizmy zapewniające spełnienie wymogów zawartych w art. 4 ust. 1, i w przypadku, gdy wdrożenie takich mechanizmów nie stanowiłoby nieproporcjonalnego obciążenia dla producenta lub dostawcy usług powiązanych.

Sporządzono w

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