

## I

(Akty ustawodawcze)

## ROZPORZĄDZENIA

### 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)

(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 <sup>(1)</sup>,

uwzględniając opinię Komitetu Regionów <sup>(2)</sup>,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą <sup>(3)</sup>,

a także mając na uwadze, co następuje:

- (1) Usługi cyfrowe ogółem, a w szczególności platformy internetowe, odgrywają coraz większą rolę w gospodarce, w szczególności na rynku wewnętrznym, ponieważ umożliwiają przedsiębiorstwom docieranie do użytkowników w całej Unii, ułatwiają handel transgraniczny i stwarzają zupełnie nowe możliwości rynkowe wielu przedsiębiorstwom w Unii z korzyścią dla unijnych konsumentów.
- (2) Jednocześnie należące do tych usług cyfrowych podstawowe usługi platformowe charakteryzują się wieloma cechami, które mogą być wykorzystywane przez przedsiębiorstwa świadczące takie usługi. Przykładem takich cech podstawowych usług platformowych są ogromne korzyści skali, które często wynikają z niemal zerowych kosztów krańcowych pozyskiwania użytkowników biznesowych lub użytkowników końcowych. Inne takie cechy podstawowych usług platformowych to bardzo silne efekty sieciowe, zdolność łączenia wielu użytkowników biznesowych z wieloma użytkownikami końcowymi dzięki wielostronności tych usług, znaczny stopień zależności zarówno użyt-

<sup>(1)</sup> Dz.U. C 286 z 16.7.2021, s. 64.

<sup>(2)</sup> Dz.U. C 440 z 29.10.2021, s. 67.

<sup>(3)</sup> Stanowisko Parlamentu Europejskiego z dnia 5 lipca 2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 18 lipca 2022 r.

kowników biznesowych, jak i użytkowników końcowych, efekty uzależnienia od jednego dostawcy, brak możliwości korzystania przez użytkowników końcowych z wielu platform (*multi-homing*) do tego samego celu, struktura zintegrowana pionowo oraz korzyści wynikające z dostępu do danych. Wszystkie te cechy w połączeniu z nieuczciwymi praktykami przedsiębiorstw świadczących podstawowe usługi platformowe mogą w znacznym stopniu osłabić kontestowalność podstawowych usług platformowych, jak również wpłynąć na uczciwość stosunków handlowych między przedsiębiorstwami świadczącymi takie usługi a ich użytkownikami biznesowymi i użytkownikami końcowymi. W praktyce prowadzi to do szybkiego i potencjalnie znacznego zmniejszenia wyboru, jakim dysponują użytkownicy biznesowi i użytkownicy końcowi, co w rezultacie może sprawić, że dostawca tych usług uzyska status tzw. strażnika dostępu. Jednocześnie należy stwierdzić, że usługi świadczone w celach niekomercyjnych, takie jak projekty oparte na współpracy, nie powinny być uznawane za podstawowe usługi platformowe do celów niniejszego rozporządzenia.

- (3) Pojawiła się niewielka liczba dużych przedsiębiorstw świadczących podstawowe usługi platformowe o znaczącej sile gospodarczej, co kwalifikowałoby je do wskazania ich jako strażników dostępu na podstawie niniejszego rozporządzenia. Zazwyczaj cechuje je zdolność łączenia – za pośrednictwem świadczonych usług – wielu użytkowników biznesowych z wieloma użytkownikami końcowymi, co z kolei umożliwia im wykorzystywanie przewagi, wynikającej na przykład z dostępu do dużych ilości danych, nabytej w jednym obszarze działalności w innym obszarze działalności. Niektóre z tych przedsiębiorstw sprawują kontrolę nad całymi ekosystemami platform w gospodarce cyfrowej i ze względów strukturalnych niezwykle trudno jest zakwestionować lub podważyć ich pozycję istniejącą lub nowym podmiotom rynkowym, niezależnie od tego, na ile mogłyby one być innowacyjne i wydajne. Kontestowalność jest ograniczona w szczególności ze względu na istnienie bardzo wysokich barier wejścia na rynek lub wyjścia z rynku, w tym wysokich kosztów inwestycji, których odzyskanie jest niemożliwe lub utrudnione w przypadku wyjścia z rynku, oraz brak dostępu lub ograniczony dostęp do niektórych kluczowych zasobów w gospodarce cyfrowej, takich jak dane. W rezultacie wzrasta prawdopodobieństwo, że rynki bazowe nie funkcjonują prawidłowo lub że wkrótce przestaną funkcjonować prawidłowo.
- (4) Połączenie tych cech strażników dostępu może prowadzić w wielu przypadkach do poważnego zachwiania równowagi w zakresie siły przetargowej, a w konsekwencji do nieuczciwych praktyk i warunków dla użytkowników biznesowych oraz dla użytkowników końcowych podstawowych usług platformowych świadczonych przez strażników dostępu, ze szkodą dla cen, jakości, uczciwej konkurencji, wyboru i innowacyjności w sektorze cyfrowym.
- (5) W rezultacie procesy rynkowe często nie są w stanie zapewnić uczciwych wyników ekonomicznych w odniesieniu do podstawowych usług platformowych. Chociaż art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) mają zastosowanie do praktyk strażników dostępu, zakres stosowania tych postanowień ogranicza się do niektórych przypadków władzy rynkowej, na przykład dominacji na określonych rynkach oraz zachowania antykonkurencyjnego, a ich egzekwowanie następuje *ex post* i wymaga dogłębnego zbadania w każdym przypadku z osobna często bardzo złożonego stanu faktycznego. Ponadto obowiązujące prawo Unii nie uwzględnia lub nie uwzględnia w sposób skuteczny wyzwań dla skutecznego funkcjonowania rynku wewnętrznego wynikających z praktyk strażników dostępu, którzy niekoniecznie mają dominującą pozycję w rozumieniu prawa konkurencji.
- (6) Strażnicy dostępu wywierają znaczący wpływ na rynek wewnętrzny, gdyż zapewniają dużej liczbie użytkowników biznesowych punkty dostępu umożliwiające im docieranie do użytkowników końcowych w dowolnym miejscu w Unii i na różnych rynkach. Negatywny wpływ nieuczciwych praktyk na rynek wewnętrzny oraz szczególnie słaba kontestowalność podstawowych usług platformowych, w tym negatywne skutki społeczne i gospodarcze takich nieuczciwych praktyk, skłoniły ustawodawców krajowych i sektorowe organy regulacyjne do podjęcia działań. Na poziomie krajowym przyjęto już lub zaproponowano szereg rozwiązań regulacyjnych w celu rozwiązania problemu nieuczciwych praktyk i kontestowalności usług cyfrowych lub przynajmniej w odniesieniu do niektórych z nich. Doprowadziło to do rozbieżnych rozwiązań regulacyjnych, a w ich rezultacie – do fragmentacji rynku wewnętrznego, co zwiększa ryzyko wzrostu kosztów przestrzegania przepisów ze względu na różne zbiory krajowych wymogów regulacyjnych.
- (7) W związku z tym celem niniejszego rozporządzenia jest przyczynienie się do prawidłowego funkcjonowania rynku wewnętrznego poprzez ustanowienie przepisów mających na celu zapewnienie kontestowalności i uczciwości rynków w sektorze cyfrowym w ogóle, a w szczególności dla użytkowników biznesowych i użytkowników końcowych podstawowych usług platformowych świadczonych przez strażników dostępu. Użytkownikom biznesowym i użytkownikom końcowym korzystającym z podstawowych usług platformowych świadczonych przez strażników dostępu należy zapewnić w całej Unii odpowiednie zabezpieczenia regulacyjne przed nieuczciwymi praktykami

strażników dostępu, aby ułatwić transgraniczne prowadzenie działalności gospodarczej w Unii i tym samym poprawić prawidłowe funkcjonowanie rynku wewnętrznego oraz wyeliminować istniejącą lub mogącą się pojawić fragmentację w określonych obszarach objętych niniejszym rozporządzeniem. Co więcej, chociaż strażnicy dostępu mają tendencję do obierania globalnych lub przynajmniej ogólnoeuropejskich modeli biznesowych i struktur algorytmicznych, mogą oni obierać, a w niektórych przypadkach obrali, różne warunki i praktyki biznesowe w różnych państwach członkowskich, co może prowadzić do powstania różnic w warunkach konkurencji dla użytkowników podstawowych usług platformowych świadczonych przez strażników dostępu, ze szkodą dla integracji rynku wewnętrznego.

- (8) Zbliżenie rozbieżnych przepisów krajowych umożliwi wyeliminowanie przeszkód wobec swobody świadczenia i odbioru usług, w tym usług detalicznych, na rynku wewnętrznym. Należy zatem ustanowić ukierunkowany zbiór zharmonizowanych obowiązków prawnych na poziomie Unii, aby zapewnić contestowalne i uczciwe rynki cyfrowe, na których działają strażnicy dostępu w ramach rynku wewnętrznego, z korzyścią dla całej gospodarki Unii, a ostatecznie – dla unijnych konsumentów.
- (9) Fragmentacji rynku wewnętrznego można skutecznie zapobiec jedynie wówczas, gdy państwa członkowskie nie będą mogły stosować przepisów krajowych, których zakres stosowania pokrywa się z zakresem stosowania niniejszego rozporządzenia i które służą tym samym celom co niniejsze rozporządzenie. Nie wyklucza to możliwości stosowania do strażników dostępu w rozumieniu niniejszego rozporządzenia innych przepisów krajowych, które służą innym uzasadnionym celom interesu publicznego określonym w TFUE lub które służą nadrzędnym względem interesu publicznego uznanym w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości”).
- (10) Jednocześnie, ponieważ niniejsze rozporządzenie ma na celu uzupełnienie egzekwowania prawa konkurencji, należy je stosować bez uszczerbku dla art. 101 i 102 TFUE, dla odpowiadających im krajowych reguł konkurencji i dla innych krajowych reguł konkurencji dotyczących praktyk jednostronnych, które opierają się na zindywidualizowanej ocenie pozycji rynkowych i zachowań rynkowych, w tym ich rzeczywistych lub potencjalnych skutków i dokładnego zakresu zabronionego zachowania, i które przewidują możliwość przedstawiania przez przedsiębiorstwa argumentów dotyczących wydajności i obiektywnego uzasadnienia danego zachowania, a także bez uszczerbku dla przepisów krajowych dotyczących kontroli łączenia przedsiębiorstw. Stosowanie tych reguł nie powinno jednak mieć wpływu na obowiązki nałożone na strażników dostępu na mocy niniejszego rozporządzenia oraz ich jednolite i skuteczne stosowanie na rynku wewnętrznym.
- (11) Art. 101 i 102 TFUE oraz odpowiadające im krajowe reguły konkurencji dotyczące antykonkurencyjnych praktyk wielostronnych i jednostronnych, jak również kontroli łączenia przedsiębiorstw, mają na celu ochronę niezakłóconej konkurencji na rynku. Niniejsze rozporządzenie służy osiągnięciu celu, który ma charakter uzupełniający względem celu polegającego na ochronie niezakłóconej konkurencji na dowolnym rynku, w rozumieniu prawa konkurencji, lecz jest różny od tego celu, a mianowicie służy zapewnieniu, aby rynki, na których działają strażnicy dostępu, były i pozostały contestowalne i uczciwe, niezależnie od rzeczywistych, potencjalnych lub domniemych skutków praktyki danego strażnika dostępu objętego niniejszym rozporządzeniem dla konkurencji na danym rynku. Niniejsze rozporządzenie ma zatem na celu ochronę innego interesu prawnego niż interes chroniony tymi regułami i powinno mieć ono zastosowanie bez uszczerbku dla stosowania tych reguł.
- (12) Niniejsze rozporządzenie powinno również mieć zastosowanie bez uszczerbku dla przepisów wynikających z innych aktów prawa Unii regulujących niektóre aspekty świadczenia usług objętych niniejszym rozporządzeniem, w szczególności rozporządzeń Parlamentu Europejskiego i Rady (UE) 2016/679 <sup>(4)</sup> i (UE) 2019/1150 <sup>(5)</sup> oraz rozporządzenia w sprawie jednolitego rynku usług cyfrowych, a także dyrektyw Parlamentu Europejskiego

<sup>(4)</sup> 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).

<sup>(5)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.U. L 186 z 11.7.2019, s. 57).

i Rady 2002/58/WE<sup>(6)</sup>, 2005/29/WE<sup>(7)</sup>, 2010/13/UE<sup>(8)</sup>, (UE) 2015/2366<sup>(9)</sup>, (UE) 2019/790<sup>(10)</sup> i (UE) 2019/882<sup>(11)</sup> oraz dyrektywy Rady 93/13/EWG<sup>(12)</sup>, jak również przepisów krajowych mających na celu egzekwowanie lub wdrożenie tych aktów prawnych Unii.

- (13) Słaba kontestowalność i nieuczciwe praktyki w sektorze cyfrowym to problem, który w przypadku niektórych usług cyfrowych występuje częściej i jest bardziej wyraźny. Dotyczy to w szczególności szeroko rozpowszechnionych i powszechnie wykorzystywanych usług cyfrowych, które przeważnie pośredniczą między użytkownikami biznesowymi a użytkownikami końcowymi w sposób bezpośredni i które najczęściej charakteryzują się takimi cechami, jak ogromne korzyści skali, bardzo silne efekty sieciowe, zdolność łączenia wielu użytkowników biznesowych z wieloma użytkownikami końcowymi dzięki wielostronności tych usług, efekty uzależnienia od jednego dostawcy, brak możliwości korzystania z wielu platform (*multi-homing*), czy struktura zintegrowana pionowo. Często istnieje tylko jedno duże przedsiębiorstwo świadczące takie usługi cyfrowe lub bardzo ograniczona liczba takich przedsiębiorstw. Przedsiębiorstwa takie najczęściej zaczynają odgrywać rolę strażników dostępu dla użytkowników biznesowych i użytkowników końcowych, co ma poważne konsekwencje. W szczególności zyskują one zdolność łatwego ustalania warunków handlowych w sposób jednostronny i ze szkodą dla swoich użytkowników biznesowych i użytkowników końcowych. W związku z tym należy skoncentrować się wyłącznie na tych usługach cyfrowych, z których najpowszechniej korzystają użytkownicy biznesowi i użytkownicy końcowi, oraz na tych, w przypadku których obawy dotyczące słabej kontestowalności i nieuczciwych praktyk ze strony strażników dostępu są wyraźniejsze i bardziej naglące z punktu widzenia rynku wewnętrznego.
- (14) W szczególności usługi pośrednictwa internetowego, wyszukiwarki internetowe, systemy operacyjne, internetowe serwisy społecznościowe, usługi platformy udostępniania wideo, usługi łączności interpersonalnej niewykorzystujące numerów, usługi przetwarzania w chmurze, wirtualni asystenci, przeglądarki internetowe i internetowe usługi reklamowe, w tym usługi pośrednictwa reklamowego, mogą mieć wpływ na dużą liczbę użytkowników końcowych i przedsiębiorstw, co pociąga za sobą ryzyko nieuczciwych praktyk biznesowych. W związku z tym należy je uwzględnić w definicji podstawowych usług platformowych i objąć zakresem stosowania niniejszego rozporządzenia. Usługi pośrednictwa internetowego mogą również występować w dziedzinie usług finansowych i mogą pośredniczyć w świadczeniu usług lub być wykorzystywane do świadczenia usług, których niewyczerpujący wykaz zawiera załącznik II do dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535<sup>(13)</sup>. Do celów niniejszego rozporządzenia definicja podstawowych usług platformowych powinna być neutralna pod względem technologicznym i z założenia obejmować usługi świadczone na różne sposoby i na różnych urządzeniach lub poprzez różne urządzenia, jak w przypadku telewizji hybrydowej lub usług cyfrowych wbudowanych w pojazdy. W pewnych okolicznościach pojęcie użytkowników końcowych powinno obejmować użytkowników, których tradycyjnie uznaje się za użytkowników biznesowych, ale którzy w danej sytuacji nie korzystają z podstawowych usług platformowych w celu dostarczania towarów lub świadczenia usług innym użytkownikom końcowym, takich jak na przykład przedsiębiorstwa korzystające z usług przetwarzania w chmurze do własnych celów.

<sup>(6)</sup> 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 (Dz.U. L 201 z 31.7.2002, s. 37).

<sup>(7)</sup> 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).

<sup>(8)</sup> Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.U. L 95 z 15.4.2010, s. 1).

<sup>(9)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35).

<sup>(10)</sup> 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).

<sup>(11)</sup> 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).

<sup>(12)</sup> Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz.U. L 95 z 21.4.1993, s. 29).

<sup>(13)</sup> Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

- (15) Fakt, że usługa cyfrowa kwalifikuje się jako podstawowa usługa platformowa, nie budzi sam w sobie wystarczająco poważnych obaw dotyczących kontestowalności lub nieuczciwych praktyk. Obawy takie pojawiają się dopiero wtedy, gdy podstawowa usługa platformowa stanowi ważny punkt dostępu i jest obsługiwana przez przedsiębiorstwo wywierające znaczący wpływ na rynek wewnętrzny oraz mające ugruntowaną i trwałą pozycję lub przez przedsiębiorstwo, co do którego można przewidzieć, że zajmie taką pozycję w niedalekiej przyszłości. W związku z tym ukierunkowany zbiór zharmonizowanych przepisów zawartych w niniejszym rozporządzeniu powinien mieć zastosowanie wyłącznie do przedsiębiorstw wskazanych na podstawie tych trzech obiektywnych kryteriów oraz wyłącznie do tych świadczonych przez nie podstawowych usług platformowych, które indywidualnie stanowią dla użytkowników biznesowych ważny punkt dostępu umożliwiający docieranie do użytkowników końcowych. To, że istnieje możliwość, iż dane przedsiębiorstwo świadczące podstawowe usługi platformowe pełni rolę pośrednika nie tylko między użytkownikami biznesowymi a użytkownikami końcowymi, lecz także między różnymi użytkownikami końcowymi, na przykład w przypadku usług łączności interpersonalnej niewykorzystujących numerów, nie powinno wykluczać stwierdzenia, że takie przedsiębiorstwo jest lub może być ważnym punktem dostępu umożliwiającym użytkownikom biznesowym docieranie do użytkowników końcowych.
- (16) Aby zapewnić skuteczne stosowanie niniejszego rozporządzenia w odniesieniu do przedsiębiorstw świadczących podstawowe usługi platformowe, które z największym prawdopodobieństwem spełnią te obiektywne wymogi, oraz tam, gdzie nieuczciwe praktyki osłabiające kontestowalność są najbardziej rozpowszechnione i mają największy wpływ, Komisja powinna mieć możliwość bezpośredniego wskazywania jako strażników dostępu tych przedsiębiorstw świadczących podstawowe usługi platformowe, które osiągnęły określone progi ilościowe. Takie przedsiębiorstwa powinny w każdym przypadku podlegać szybkiemu procesowi wskazania, który powinien się rozpocząć z chwilą rozpoczęcia stosowania niniejszego rozporządzenia.
- (17) Fakt, że dane przedsiębiorstwo uzyskuje bardzo wysoki obrót w Unii oraz że świadczy podstawową usługę platformową w co najmniej trzech państwach członkowskich, stanowi wyraźną wskazówkę, że przedsiębiorstwo to wywiera znaczący wpływ na rynek wewnętrzny. Jest tak również wówczas, gdy przedsiębiorstwo świadczące podstawową usługę platformową w co najmniej trzech państwach członkowskich ma bardzo wysoką kapitalizację rynkową lub równoważną rzeczywistą wartość rynkową. W związku z tym należy domniemywać, że przedsiębiorstwo świadczące podstawową usługę platformową wywiera znaczący wpływ na rynek wewnętrzny, gdy świadczy ono podstawową usługę platformową w co najmniej trzech państwach członkowskich oraz gdy obrót uzyskiwany przez jego grupę w Unii jest równy określonej wysokiej wartości progowej lub go przekracza albo gdy kapitalizacja rynkowa grupy jest równa określonej wysokiej wartości bezwzględnej lub ją przekracza. W przypadku przedsiębiorstw świadczących podstawowe usługi platformowe, które należą do przedsiębiorstw nienotowanych na rynku regulowanym, jako wartość referencyjną należy stosować równoważną rzeczywistą wartość rynkową. Komisja powinna mieć możliwość korzystania ze swoich uprawnień do przyjmowania aktów delegowanych, aby opracować obiektywną metodę obliczania tej wartości.

Wysoki obrót uzyskiwany przez grupę w Unii w połączeniu z określoną wartością progową liczby użytkowników podstawowych usług platformowych w Unii świadczy o stosunkowo dużej zdolności monetyzacji tych użytkowników. Wysoka kapitalizacja rynkowa w odniesieniu do tej samej wartości progowej liczby użytkowników w Unii odzwierciedla stosunkowo duży potencjał w zakresie monetyzacji tych użytkowników w niedalekiej przyszłości. Potencjał w zakresie monetyzacji jest z kolei co do zasady odzwierciedleniem pełnienia przez dane przedsiębiorstwa funkcji punktu dostępu. Oba te wskaźniki świadczą ponadto o zdolności finansowej danych przedsiębiorstw, w tym o ich zdolności w zakresie wykorzystania swojego dostępu do rynków finansowych w celu wzmocnienia swojej pozycji. Może się tak zdarzyć na przykład wówczas, gdy ten uprzywilejowany dostęp zostanie wykorzystany do nabycia innych przedsiębiorstw, a, jak wykazano, taki uprzywilejowany dostęp może z kolei negatywnie wpływać na innowacje. Kapitalizacja rynkowa może również odzwierciedlać oczekiwaną przyszłą pozycję i wpływ na rynek wewnętrzny danych przedsiębiorstw pomimo potencjalnie stosunkowo niskiego obecnego obrotu. Wartość kapitalizacji rynkowej powinna być wyznaczana w oparciu o poziom, który odzwierciedla średnią kapitalizację rynkową największych przedsiębiorstw notowanych na rynku regulowanym w Unii z odpowiedniego okresu.

- (18) O ile kapitalizacja rynkowa na poziomie równym progowi lub powyżej progu w ostatnim roku obrotowym powinna pozwalać na domniemanie, że dane przedsiębiorstwo świadczące podstawowe usługi platformowe wywiera znaczący wpływ na rynek wewnętrzny, o tyle należy uznać, że kapitalizacja rynkowa przedsiębiorstwa świadczącego podstawowe usługi platformowe utrzymująca się na poziomie równym progowi lub powyżej progu przez co najmniej trzy lata jeszcze bardziej wzmacnia takie domniemanie.

- (19) Może występować natomiast szereg czynników dotyczących kapitalizacji rynkowej, które wymagałyby dogłębnej oceny w celu ustalenia, czy należy uznać, że przedsiębiorstwo świadczące podstawowe usługi platformowe wywiera znaczący wpływ na rynek wewnętrzny. Może tak być w przypadku, gdy w poprzednich latach obrotowych kapitalizacja rynkowa przedsiębiorstwa świadczącego podstawowe usługi platformowe była na poziomie znacznie poniżej progów, a zmienność jego kapitalizacji rynkowej w obserwowanym okresie była nieproporcjonalna do ogólnej zmienności rynku akcji lub jego trajektoria kapitalizacji rynkowej w stosunku do tendencji rynkowych nie była spójna z szybkim i jednokierunkowym wzrostem.
- (20) Posiadanie bardzo dużej liczby użytkowników biznesowych, którzy są zależni od podstawowej usługi platformowej, aby docierać do bardzo dużej liczby aktywnych miesięcznie użytkowników końcowych, umożliwia przedsiębiorstwu świadczącemu tę usługę wpływanie – z korzyścią dla siebie – na działalność znacznej części użytkowników biznesowych oraz zasadniczo wskazuje na to, że przedsiębiorstwo to stanowi ważny punkt dostępu. Należy ustalić odpowiednie poziomy tych wartości stanowiące znaczny odsetek całej ludności Unii, jeżeli chodzi o użytkowników końcowych, oraz ogółu przedsiębiorstw korzystających z podstawowych usług platformowych, aby określić próg dotyczący użytkowników biznesowych. Aktywnych użytkowników końcowych i aktywnych użytkowników biznesowych należy identyfikować i obliczać ich liczbę w taki sposób, aby odpowiednio odzwierciedlić rolę i zasięg danej podstawowej usługi platformowej. Aby zagwarantować strażnikom dostępu pewność prawa, w załączniku do niniejszego rozporządzenia należy wskazać elementy służące określeniu liczby aktywnych użytkowników końcowych i aktywnych użytkowników biznesowych poszczególnych podstawowych usług platformowych. Na takie elementy mogą mieć wpływ rozwój technologiczny i inne zmiany. Komisja powinna zatem być uprawniona do przyjmowania aktów delegowanych w celu zmiany niniejszego rozporządzenia poprzez aktualizację metodyki i wykazu wskaźników stosowanych do określenia liczby aktywnych użytkowników końcowych i aktywnych użytkowników biznesowych.
- (21) Ugruntowana i trwała pozycja w zakresie prowadzonej działalności lub przewidywalne zajęcie takiej pozycji w przyszłości występuje zwłaszcza wtedy, gdy kontestowalność pozycji przedsiębiorstwa świadczącego daną podstawową usługę platformową jest ograniczona. Może się tak zdarzyć, gdy przedsiębiorstwo to świadczy podstawową usługę platformową w co najmniej trzech państwach członkowskich na rzecz bardzo dużej liczby użytkowników biznesowych i użytkowników końcowych przez okres co najmniej 3 lat.
- (22) Na takie progi mogą mieć wpływ zmiany na rynku i rozwój technologiczny. Komisja powinna być zatem uprawniona do przyjmowania aktów delegowanych w celu określenia metodyki ustalania, czy osiągnięte zostały progi ilościowe, oraz – w razie potrzeby – w celu regularnego dostosowywania tej metodyki do zmian na rynku i rozwoju technologicznego. Takie akty delegowane nie powinny zmieniać progów ilościowych określonych w niniejszym rozporządzeniu.
- (23) Przedsiębiorstwo świadczące podstawowe usługi platformowe powinno, w wyjątkowych okolicznościach, mieć możliwość obalenia domniemania dotyczącego wywierania przez nie znaczącego wpływu na rynek wewnętrzny, poprzez wykazanie, że choć osiągnęło ono progi ilościowe określone w niniejszym rozporządzeniu, to nie spełnia wymogów do celów wskazania go jako strażnika dostępu. Ciężar przedstawienia dowodu na to, że domniemanie wynikające z osiągnięcia progów ilościowych nie powinno mieć zastosowania, powinien spoczywać na tym przedsiębiorstwie. Komisja, oceniając przedstawione jej dowody i argumenty, powinna uwzględniać jedynie te elementy, które są bezpośrednio związane z kryteriami ilościowymi, czyli z wpływem przedsiębiorstwa świadczącego podstawowe usługi platformowe na rynek wewnętrzny, poza przychodami lub kapitalizacją rynkową, takie jak wielkość przedsiębiorstwa w wartościach bezwzględnych i liczba państw członkowskich, w których przedsiębiorstwo to jest obecne; to, o ile liczba faktycznych użytkowników biznesowych i użytkowników końcowych przekracza wartości progowe, i znaczenie podstawowej usługi platformowej przedsiębiorstwa z uwzględnieniem ogólnej skali działalności odpowiedniej podstawowej usługi platformowej; oraz liczba lat, w których progi zostały osiągnięte.

Uzasadnienia ze względów gospodarczych oparte na argumentach związanych z definicją rynku lub wykazaniem przyrostów wydajności wynikających z konkretnego rodzaju postępowania przedsiębiorstwa świadczącego podstawowe usługi platformowe nie powinny być uwzględniane, ponieważ nie są one istotne w kontekście wskazywania jako strażnika dostępu. Jeżeli przedstawione argumenty nie są dostatecznie uzasadnione, ponieważ nie podważają w wyraźny sposób przedmiotowego domniemania, Komisja powinna mieć możliwość odrzucenia tych argumentów w terminie 45 dni roboczych przewidzianym w odniesieniu do wskazania. Komisja powinna mieć możliwość podjęcia decyzji na podstawie dostępnych informacji o progach ilościowych, w przypadku gdy przedsiębiorstwo świadczące podstawowe usługi platformowe utrudnia badanie, nie stosując się do środków podjętych przez Komisję w ramach badania.

- (24) W przypadku przedsiębiorstw świadczących podstawowe usługi platformowe, które nie osiągnęły wszystkich progów ilościowych, należy przeprowadzić ocenę, czy nie pełnią one roli strażnika dostępu w świetle ogólnych obiektywnych wymogów – dotyczących znaczącego wpływu na rynek wewnętrzny, działania jako ważny punkt dostępu dla użytkowników biznesowych umożliwiające docieranie do użytkowników końcowych oraz czerpania korzyści z ugruntowanej i trwałej pozycji w zakresie prowadzonej działalności lub możliwości przewidzenia, że osiągną one taką pozycję w niedalekiej przyszłości. Jeżeli przedsiębiorstwo świadczące podstawowe usługi platformowe jest średnim lub małym przedsiębiorstwem lub mikroprzedsiębiorstwem, w ramach oceny należy starannie uwzględnić to, czy takie przedsiębiorstwo byłoby w stanie w znaczny sposób osłabić kontestowalność podstawowych usług platformowych, gdyż niniejsze rozporządzenie skierowane jest przede wszystkim do dużych przedsiębiorstw o znacznej sile gospodarczej, a nie do średnich i małych przedsiębiorstw czy mikroprzedsiębiorstw.
- (25) Ocenę taką można przeprowadzić jedynie w świetle badania rynku, biorąc pod uwagę jednocześnie progi ilościowe. Przeprowadzając ocenę, Komisja powinna skoncentrować się na celach polegających na zachowaniu i wspieraniu innowacyjności i jakości produktów i usług cyfrowych, stopnia, w jakim ceny są uczciwe i konkurencyjne, oraz stopnia, w jakim jakość dla użytkowników biznesowych i użytkowników końcowych jest lub pozostaje wysoka, a wybór – duży. Można uwzględnić elementy specyficzne dla odpowiednich przedsiębiorstw świadczących podstawowe usługi platformowe, takie jak ogromne korzyści skali lub zakresu, bardzo silne efekty sieciowe, korzyści wynikające z dostępu do danych, zdolność łączenia wielu użytkowników biznesowych z wieloma użytkownikami końcowymi dzięki wielostronności tych usług, efekty uzależnienia od jednego dostawcy, brak możliwości korzystania z wielu platform (*multi-homing*), struktura korporacyjna mająca formę konglomeratu lub struktura zintegrowana pionowo. Ponadto bardzo wysoka kapitalizacja rynkowa, bardzo wysoki stosunek wartości kapitału własnego do zysku lub bardzo wysoki obrót uzyskany z tytułu użytkowników końcowych pojedynczej podstawowej usługi platformowej mogą być wykorzystywane jako elementy wskazujące na potencjał takich przedsiębiorstw w zakresie wykorzystywania swojej pozycji oraz na występowanie zjawiska przechyłu rynkowego na rzecz takich przedsiębiorstw. Oprócz kapitalizacji rynkowej również wysokie względne stopy wzrostu stanowią przykład dynamicznych parametrów, które mają szczególne znaczenie dla identyfikowania przedsiębiorstw świadczących podstawowe usługi platformowe, w przypadku których można przewidywać, że ich pozycja rynkowa stanie się ugruntowana i trwała. W przypadku gdy przedsiębiorstwo świadczące podstawowe usługi platformowe znacznie utrudnia badanie, nie stosując się do środków podjętych przez Komisję w ramach badania, Komisja powinna mieć możliwość wyciągnięcia wniosków niekorzystnych dla tego przedsiębiorstwa na podstawie dostępnych faktów i wydania w oparciu o nie decyzji.
- (26) Do przedsiębiorstw świadczących podstawowe usługi platformowe, w przypadku których można przewidzieć, że w niedalekiej przyszłości zajmą ugruntowaną i trwałą pozycję, powinien mieć zastosowanie szczególnie podzbiór przepisów. Te same specyficzne cechy podstawowych usług platformowych sprawiają, że zachodzi ryzyko przechyłu rynkowego: gdy przedsiębiorstwo świadczące podstawową usługę platformową uzyska określoną przewagę nad rywalami lub potencjalnymi konkurentami pod względem skali lub znaczenia jako pośrednik, jego pozycja może stać się niepodważalna, a sytuacja może rozwinąć się na tyle, że prawdopodobnie w niedalekiej przyszłości pozycja ta stanie się ugruntowana i trwała. Przedsiębiorstwa mogą próbować spowodować taki przechył rynkowy i stawać się strażnikami dostępu, wykorzystując niektóre z nieuczciwych warunków i praktyk regulowanych niniejszym rozporządzeniem. W takiej sytuacji odpowiednia wydaje się interwencja, zanim przechył rynkowy stanie się nieodwracalny.
- (27) Taka wczesna interwencja powinna być jednak ograniczona do nałożenia wyłącznie tych obowiązków, które są niezbędne i odpowiednie do zapewnienia, aby przedmiotowe usługi pozostały kontestowalne, i do umożliwienia uniknięcia uzasadnionego ryzyka związanego z nieuczciwymi warunkami i praktykami. Realizacji tego celu mają służyć zwłaszcza obowiązki uniemożliwiające przedsiębiorstwu świadczącemu podstawowe usługi platformowe zajęcie ugruntowanej i trwałej pozycji w zakresie prowadzonej działalności, między innymi obowiązki uniemożliwiające mu wykorzystywanie swojej pozycji oraz obowiązki, których celem jest ułatwienie zmiany i korzystania z wielu platform (*multi-homing*). Aby zapewnić proporcjonalność, Komisja powinna ponadto stosować spośród tego podzbioru obowiązków jedynie te, które są niezbędne i proporcjonalne do osiągnięcia celów niniejszego rozporządzenia, oraz powinna dokonywać regularnego przeglądu, aby ustalić, czy takie obowiązki należy utrzymać, znieść lub dostosować.
- (28) Stosowanie wyłącznie tych obowiązków, które są niezbędne i proporcjonalne do osiągnięcia celów niniejszego rozporządzenia, powinno umożliwić Komisji przeprowadzanie interwencji na czas i w skuteczny sposób, przy jednoczesnym pełnym poszanowaniu proporcjonalności rozważanych środków. Powinno to również wzmocnić zaufanie istniejących lub potencjalnych uczestników rynku co do kontestowalności i uczciwości danych usług.
- (29) Strażnicy dostępu powinni wypełniać obowiązki ustanowione w niniejszym rozporządzeniu w odniesieniu do każdej z podstawowych usług platformowych wymienionych w odpowiedniej decyzji o wskazaniu. Obowiązki powinny mieć zastosowanie z uwzględnieniem, w stosownych przypadkach, konglomeratowego charakteru pozycji strażników dostępu. Ponadto Komisja powinna mieć możliwość nałożenia na strażnika dostępu, w drodze decyzji, środków

wykonawczych. Te środki wykonawcze powinny zostać zaprojektowane w efektywny sposób, z uwzględnieniem cech podstawowych usług platformowych i możliwego ryzyka obchodzenia obowiązków oraz zgodnie z zasadą proporcjonalności i z poszanowaniem praw podstawowych odnośnych przedsiębiorstw oraz osób trzecich.

- (30) Bardzo szybko zmieniający się i złożony pod względem technologicznym charakter podstawowych usług platformowych wymaga dokonywania regularnego przeglądu statusu strażników dostępu, w tym tych, w przypadku których przewiduje się, że w niedalekiej przyszłości zajmą ugruntowaną i trwałą pozycję w zakresie prowadzonej działalności. Aby zapewnić wszystkim uczestnikom rynku, w tym strażnikom dostępu, wymaganą pewność co do mających zastosowanie obowiązków prawnych, konieczne jest wyznaczenie terminu na przeprowadzanie takich regularnych przeglądów. Ważne jest również przeprowadzanie takich przeglądów regularnie, nie rzadziej niż co 3 lata. Ponadto ważne jest wyjaśnienie, że nie każda zmiana stanu faktycznego, na podstawie którego przedsiębiorstwo świadczące podstawowe usługi platformowe zostało wskazane jako strażnik dostępu, powinna wymagać zmiany decyzji o wskazaniu. Zmiana decyzji będzie konieczna jedynie wtedy, gdy zmiana stanu faktycznego prowadzi również do zmiany oceny. Stwierdzenie, czy tak się stało, powinno opierać się na ocenie stanu faktycznego i okoliczności.
- (31) Aby zabezpieczyć kontestowalność i uczciwość podstawowych usług platformowych świadczonych przez strażników dostępu, konieczne jest ustanowienie w sposób jasny i jednoznaczny zbioru zharmonizowanych przepisów dotyczących tych usług. Takie przepisy są potrzebne, aby zniwelować ryzyko dotyczące szkodliwych skutków praktyk stosowanych przez strażników dostępu, i byłyby korzystne dla środowiska biznesowego, w którym świadczone są przedmiotowe usługi, dla użytkowników oraz – ostatecznie – dla całego społeczeństwa. Obowiązki dotyczą tych praktyk, które biorąc pod uwagę cechy sektora cyfrowego uznaje się za osłabiające kontestowalność lub nieuczciwe, oraz do tych praktyk, które mają szczególnie negatywny bezpośredni wpływ na użytkowników biznesowych i użytkowników końcowych. Należy umożliwić szczególne uwzględnienie w ramach obowiązków ustanowionych w niniejszym rozporządzeniu charakteru świadczonych podstawowych usług platformowych. Obowiązki ustanowione w niniejszym rozporządzeniu powinny nie tylko zapewniać kontestowalność i uczciwość w odniesieniu do podstawowych usług platformowych wymienionych w decyzji o wskazaniu, ale także w odniesieniu do innych cyfrowych produktów i usług, w przypadku których strażnicy dostępu wykorzystują swoją funkcję punktu dostępu i które są często dostarczane lub świadczone wraz z podstawowymi usługami platformowymi lub wspierają takie usługi.
- (32) Do celów niniejszego rozporządzenia kontestowalność powinna odnosić się do zdolności przedsiębiorstw do skutecznego pokonywania barier wejścia i rozszerzania działalności oraz do podważania pozycji strażnika dostępu na podstawie zalet oferowanych przez te przedsiębiorstwa produktów i usług. Cechy podstawowych usług platformowych w sektorze cyfrowym, takie jak efekty sieciowe, silne korzyści skali oraz korzyści wynikające z danych, ograniczyły kontestowalność tych usług oraz powiązanych z nimi ekosystemów. Taka słaba kontestowalność zmniejsza bodźce dla strażników dostępu, ich użytkowników biznesowych, konkurentów i klientów do wprowadzania innowacji i ulepszania produktów i usług, co wpływa negatywnie na potencjał innowacyjny szerzej pojętej gospodarki platform internetowych. Kontestowalność usług w sektorze cyfrowym może być ograniczona także wtedy, gdy w przypadku podstawowej usługi platformowej istnieje więcej niż jeden strażnik dostępu. W niniejszym rozporządzeniu należy zatem zakazać niektórych praktyk stosowanych przez strażników dostępu, które mogą zwiększać bariery wejścia lub rozszerzania działalności, oraz nałożyć na strażników dostępu pewne obowiązki, które przyczynią się do obniżenia tych barier. Obowiązki powinny również odnosić się do sytuacji, w których pozycja strażnika dostępu jest ugruntowana do tego stopnia, że konkurencja między platformami jest nieskuteczna w perspektywie krótkoterminowej, co oznacza, że konkurencję taką należy stworzyć lub zwiększyć.
- (33) Do celów niniejszego rozporządzenia nieuczciwość powinna odnosić się do sytuacji braku równowagi między prawami a obowiązkami użytkowników biznesowych, w której strażnik dostępu uzyskuje nieproporcjonalną przewagę. Uczestnicy rynku, w tym użytkownicy biznesowi podstawowych usług platformowych i alternatywni dostawcy usług świadczonych wraz z takimi podstawowymi usługami platformowymi lub wspierających takie usługi, powinni być w stanie czerpać odpowiednio korzyści wynikające z ich wysiłków innowacyjnych lub innego rodzaju wysiłków. Strażnicy dostępu, ze względu na pełnią przez nich funkcję punktu dostępu i większą siłę przetargową, mogą dopuszczać się zachowań uniemożliwiających innym uzyskanie pełnych korzyści z ich własnego wkładu oraz jednostronnie nakładać nierównoważne warunki korzystania z ich podstawowych usług platformowych lub usług świadczonych wraz z ich podstawowymi usługami platformowymi lub wspierających takie usługi. Takiego braku równowagi nie wyklucza fakt, że strażnik dostępu oferuje daną usługę nieodpłatnie określonej grupie użytkowników; brak równowagi może również polegać na wykluczeniu lub dyskryminowaniu użytkowników biznesowych, w szczególności jeżeli świadczą oni usługi konkurencyjne względem usług świadczonych przez strażnika dostępu. W niniejszym rozporządzeniu należy zatem nałożyć na strażników dostępu obowiązki mające zaradzić takim zachowaniom.



- (34) Kontestowalność i uczciwość są ze sobą ściśle powiązane. Brak kontestowalności lub słaba kontestowalność w przypadku określonej usługi może umożliwić strażnikowi dostępu stosowanie nieuczciwych praktyk. Podobnie nieuczciwe praktyki strażnika dostępu mogą ograniczyć użytkownikom biznesowym lub innym podmiotom możliwość kwestionowania pozycji strażnika dostępu. W związku z tym określony obowiązek ustanowiony w niniejszym rozporządzeniu może dotyczyć obu tych elementów.
- (35) Obowiązki ustanowione w niniejszym rozporządzeniu są zatem konieczne, aby zaradzić określonym obawom dotyczącym porządku publicznego; uwzględniając potrzebę ochrony porządku publicznego, ochrony prywatności i zwalczania oszukańczych i wprowadzających w błąd praktyk handlowych, nie można osiągnąć tego samego rezultatu za pomocą innych, mniej restrykcyjnych środków.
- (36) Strażnicy dostępu często bezpośrednio zbierają dane osobowe użytkowników końcowych do celów świadczenia internetowych usług reklamowych, gdy użytkownicy końcowi korzystają ze stron internetowych i aplikacji oferowanych przez osoby trzecie. Osoby trzecie również przekazują strażnikom dostępu dane osobowe swoich użytkowników końcowych, aby korzystać z niektórych usług świadczonych przez strażników dostępu w ramach ich podstawowych usług platformowych, takich jak usługi tworzenia grup niestandardowych odbiorców. Przetwarzanie – do celów świadczenia internetowych usług reklamowych – danych osobowych pochodzących od osób trzecich korzystających z podstawowych usług platformowych daje strażnikom dostępu potencjalną przewagę wynikającą z akumulacji danych, tym samym podnosząc bariery wejścia. Dzieje się tak, gdyż strażnicy dostępu przetwarzają dane osobowe pochodzące od znacznie większej liczby osób trzecich niż ma to miejsce w przypadku innych przedsiębiorstw. Podobną przewagę uzyskują oni w wyniku (i) łączenia danych osobowych użytkowników końcowych, które to dane zebrano za pośrednictwem podstawowej usługi platformowej, z danymi zebranymi za pośrednictwem innych usług, (ii) wykorzystywania danych osobowych zebranych za pośrednictwem podstawowej usługi platformowej w ramach innych usług świadczonych oddzielnie przez strażnika dostępu, zwłaszcza usług innych niż usługi świadczone wraz z odpowiednią podstawową usługą platformową lub wspierające taką usługę, i odwrotnie – wykorzystywania danych osobowych zebranych za pośrednictwem takich innych usług w ramach podstawowej usługi platformowej, lub (iii) logowania użytkowników końcowych do różnych usług świadczonych przez strażnika dostępu, po to by łączyć dane osobowe. W celu zapewnienia, aby strażnicy dostępu nie osłabiali w nieuczciwy sposób kontestowalności podstawowych usług platformowych, powinni oni dawać użytkownikom końcowym możliwość swobodnego decydowania o uczestnictwie w takich praktykach w zakresie przetwarzania danych i logowania, oferując mniej spersonalizowane, lecz równoważne rozwiązanie alternatywne oraz nie uzależniając korzystania z podstawowej usługi platformowej lub niektórych jej funkcjonalności od uzyskania zgody od użytkownika końcowego. Powinno to pozostawać bez uszczerbku dla przetwarzania danych osobowych przez strażnika dostępu lub logowania użytkowników końcowych do usługi w oparciu o podstawę prawną ustanowioną w art. 6 ust. 1 lit. c), d) i e) rozporządzenia (UE) 2016/679, lecz nie w art. 6 ust. 1 lit. b) i f) tego rozporządzenia.
- (37) Mniej spersonalizowane rozwiązanie alternatywne nie powinno mieć innego charakteru lub gorszej jakości w porównaniu z usługą świadczoną użytkownikom końcowym, którzy wyrazili zgodę, chyba że pogorszenie jakości wynika bezpośrednio z tego, że strażnik dostępu nie jest w stanie przetwarzać takich danych osobowych lub logować użytkowników końcowych do usługi. Niewyrażenie zgody nie powinno być trudniejsze od wyrażenia zgody. W przypadku gdy strażnik dostępu zwraca się o wyrażenie zgody, powinien proaktywnie przedstawiać użytkownikowi końcowemu przyjazne dla użytkownika rozwiązanie umożliwiające wyrażenie, zmianę lub cofnięcie zgody w sposób wyraźny, jasny i prosty. W szczególności zgoda powinna zostać wyrażona w drodze wyraźnego działania potwierdzającego lub oświadczenia stanowiącego dobrowolne, konkretne, świadome i jednoznaczne wyrażenie przyzwolenia przez użytkownika końcowego, zgodnie z definicją w rozporządzeniu (UE) 2016/679. W momencie wyrażania zgody, i wyłącznie w stosownych przypadkach, użytkownik końcowy powinien zostać poinformowany, że niewyrażenie zgody może prowadzić do mniej spersonalizowanej oferty, ale że poza tym podstawowa usługa platformowa pozostanie niezmieniona i że żadne funkcjonalności nie zostaną usunięte. Na zasadzie wyjątku, jeżeli nie można wyrazić zgody bezpośrednio w ramach podstawowej usługi platformowej strażnika dostępu, należy umożliwić użytkownikom końcowym wyrażenie zgody za pośrednictwem każdej korzystającej z tej podstawowej usługi platformowej usługi świadczonej przez osobę trzecią, aby zezwolić strażnikowi dostępu na przetwarzanie danych osobowych do celów świadczenia internetowych usług reklamowych.

Ponadto cofnięcie zgody powinno być równie proste co jej wyrażenie. Strażnicy dostępu nie powinni projektować, organizować lub obsługiwać swoich interfejsów internetowych w sposób, który w drodze wprowadzenia w błąd, manipulacji lub w inny sposób istotnie zakłóca lub ogranicza zdolność użytkowników końcowych do swobodnego wyrażenia zgody. W szczególności strażnikom dostępu należy zakazać skłaniania użytkowników końcowych częściej niż raz w roku do wyrażenia zgody do tego samego celu przetwarzania danych, w odniesieniu do którego nie wyrazili oni pierwotnie zgody lub ją cofnęli. Niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzenia (UE) 2016/679, w tym przepisów dotyczących jego egzekwowania, które ma pełne zastosowanie do roszczeń osób, których dane dotyczą, z tytułu naruszenia ich praw wynikających z tego rozporządzenia.

- (38) Dzieci zasługują na szczególną ochronę w odniesieniu do ich danych osobowych, w szczególności pod względem wykorzystywania ich danych osobowych do celów informacji handlowych lub tworzenia profili użytkowników. Ochrona dzieci w internecie jest jednym z istotnych celów Unii i powinna znaleźć odzwierciedlenie w stosownych przepisach prawa Unii. W związku z tym należy odpowiednio uwzględnić rozporządzenie w sprawie jednolitego rynku usług cyfrowych. Żaden z przepisów niniejszego rozporządzenia nie zwalnia strażników dostępu z obowiązku ochrony dzieci ustanowionego w mających zastosowanie przepisach prawa Unii.
- (39) W niektórych przypadkach, na przykład poprzez narzucanie warunków umownych, strażnicy dostępu mogą ograniczać użytkownikom biznesowym swoich usług pośrednictwa internetowego możliwość oferowania użytkownikom końcowym – przy wykorzystaniu innych usług pośrednictwa internetowego lub za pomocą kanałów bezpośredniej sprzedaży internetowej – produktów lub usług na korzystniejszych warunkach, w tym cenowych. W przypadku gdy takie ograniczenia dotyczą usług pośrednictwa internetowego świadczonych przez osobę trzecią, zmniejszają one kontestowalność między platformami, a w konsekwencji ograniczają użytkownikom końcowym wybór alternatywnych usług pośrednictwa internetowego. W przypadku gdy takie ograniczenia dotyczą kanałów bezpośredniej sprzedaży internetowej, zmniejszają one w nieuczciwy sposób przysługującą użytkownikom biznesowym swobodę korzystania z takich kanałów. W celu zapewnienia, aby użytkownicy biznesowi usług pośrednictwa internetowego świadczonych przez strażników dostępu mogli swobodnie wybierać alternatywne usługi pośrednictwa internetowego lub kanały bezpośredniej sprzedaży internetowej i różnicować warunki, na jakich oferują swoje produkty lub usługi użytkownikom końcowym, nie należy akceptować ograniczania przez strażników dostępu możliwości różnicowania warunków handlowych, w tym cenowych, przez użytkowników biznesowych. Powinno to dotyczyć każdego środka o równoważnym skutku, takiego jak zwiększone stawki prowizji lub usunięcie z listy ofert użytkowników biznesowych.
- (40) W celu zapobieżenia dalszemu zwiększeniu zależności użytkowników biznesowych od podstawowych usług platformowych świadczonych przez strażników dostępu i w celu promowania korzystania z wielu platform (*multi-homing*), użytkownicy biznesowi tych strażników dostępu powinni mieć swobodę promowania i wybierania kanału dystrybucji, który uważają za najbardziej odpowiedni w kontaktach z użytkownikami końcowymi, których ci użytkownicy biznesowi już pozyskali za pośrednictwem podstawowych usług platformowych świadczonych przez strażnika dostępu lub za pośrednictwem innych kanałów. Powinno to dotyczyć promowania ofert, w tym przy wykorzystaniu aplikacji użytkownika biznesowego, oraz wszelkich form porozumiewania się i zawierania umów między użytkownikami biznesowymi a użytkownikami końcowymi. Pozyskany użytkownik końcowy to użytkownik końcowy, który nawiązał już stosunek handlowy z użytkownikiem biznesowym, a strażnik dostępu, w stosownym przypadku, otrzymał, bezpośrednio lub pośrednio, wynagrodzenie od użytkownika biznesowego za ułatwienie pierwotnego pozyskania użytkownika końcowego przez użytkownika biznesowego. Takie stosunki handlowe mogą mieć charakter odpłatny lub darmowy, na przykład darmowe okresy próbne lub poziom bezpłatny dostępu do usług, i mogą zostać zawarte przy wykorzystaniu podstawowej usługi platformowej strażnika dostępu albo za pośrednictwem innego kanału. Z kolei użytkownicy końcowi również powinni mieć swobodę wyboru ofert takich użytkowników biznesowych i zawierania z nimi umów za pośrednictwem podstawowych usług platformowych strażnika dostępu, w stosownych przypadkach, albo bezpośredniego kanału dystrybucji użytkownika biznesowego lub innego pośredniego kanału, z którego taki użytkownik biznesowy korzysta.
- (41) Nie należy podważać ani ograniczać możliwości nabywania przez użytkowników końcowych treści, subskrypcji, funkcji lub innych pozycji dostępnych poza podstawowymi usługami platformowymi strażnika dostępu. W szczególności należy unikać sytuacji, w której strażnicy dostępu ograniczają użytkownikom końcowym za pośrednictwem aplikacji działającej w ramach ich podstawowej usługi platformowej dostęp do takich usług i możliwość korzystania z nich. Na przykład subskrybentom treści internetowych zakupionych poza aplikacją, sklepem z aplikacjami lub wirtualnym asystentem nie należy uniemożliwiać dostępu do takich treści internetowych w aplikacji w ramach podstawowej usługi platformowej strażnika dostępu tylko dlatego, że treści te zostały zakupione poza taką aplikacją, sklepem z aplikacjami lub wirtualnym asystentem.
- (42) W celu zabezpieczenia uczciwego środowiska handlowego i w celu ochrony kontestowalności sektora cyfrowego ważne jest, aby zabezpieczyć prawo użytkowników biznesowych i użytkowników końcowych, w tym sygnalistów, do zgłaszania obaw dotyczących nieuczciwych praktyk strażników dostępu poprzez zwracanie uwagi odpowiednich organów administracyjnych lub innych organów publicznych, w tym sądów krajowych, na wszelkie kwestie dotyczące nieprzestrzegania odpowiednich przepisów prawa Unii lub prawa krajowego. Użytkownicy biznesowi lub użytkownicy końcowi mogą na przykład chcieć złożyć skargę na różnego rodzaju nieuczciwe praktyki, takie jak dyskryminujące warunki dostępu, nieuzasadnione zamykanie kont użytkowników biznesowych lub niejasne powody usunięcia produktu z listy ofert. Należy w związku z tym zakazać wszelkich praktyk, które w jakikolwiek sposób

ograniczałyby lub utrudniały tym użytkownikom zgłaszanie obaw lub dochodzenie roszczeń, na przykład takich jak klauzule poufności zawarte w umowach lub inne określone na piśmie warunki. Zakaz ten powinien pozostawać bez uszczerbku dla prawa użytkowników biznesowych i strażników dostępu do określania w swoich umowach warunków korzystania obejmujących korzystanie z dozwolonych prawem mechanizmów rozpatrywania skarg, w tym korzystania z alternatywnych mechanizmów rozstrzygania sporów lub z jurysdykcji określonych sądów zgodnie z odpowiednimi przepisami prawa Unii i prawa krajowego. Ponadto powinno to pozostawać bez uszczerbku dla roli odgrywanej przez strażników dostępu w zwalczaniu nielegalnych treści w internecie.

- (43) Niektóre usługi świadczone wraz z odpowiednimi podstawowymi usługami platformowymi strażnika dostępu lub wspierające takie usługi, jak usługi identyfikacyjne, silniki przeglądarki internetowej, usługi płatnicze lub usługi techniczne wspierające świadczenie usług płatniczych, takie jak systemy płatności za zakupy wewnątrz aplikacji, mają zasadnicze znaczenie dla prowadzenia działalności przez użytkowników biznesowych i umożliwiają im optymalizację usług. W szczególności każda przeglądarka jest zbudowana na silniku przeglądarki internetowej, który odpowiada za kluczowe funkcjonalności przeglądarki, takie jak szybkość, niezawodność i kompatybilność z siecią. W przypadku gdy strażnicy dostępu są operatorami silników przeglądarek internetowych i narzucają korzystanie z tych silników, mogą określać funkcjonalności i normy, które będą miały zastosowanie nie tylko do ich własnych przeglądarek internetowych, ale także do przeglądarek konkurencyjnych, a przez to także do aplikacji internetowych. Strażnicy dostępu nie powinni zatem wykorzystywać swojej pozycji do wymagania od zależnych od siebie użytkowników biznesowych, aby w ramach świadczenia usług lub dostarczania produktów wykorzystywali oni usługi świadczone przez samego strażnika dostępu wraz z podstawowymi usługami platformowymi lub wspierające takie usługi. Aby uniknąć sytuacji, w której strażnicy dostępu pośrednio narzucają użytkownikom biznesowym swoje własne usługi świadczone wraz z podstawowymi usługami platformowymi lub wspierające takie usługi, należy również zakazać strażnikom dostępu wymagania od użytkowników końcowych korzystania z takich usług, gdy taki wymóg zostałby nałożony w ramach usługi świadczonej użytkownikom końcowym przez użytkownika biznesowego z wykorzystaniem podstawowej usługi platformowej strażnika dostępu. Zakaz ten ma na celu ochronę przysługującej użytkownikowi biznesowemu swobody wyboru usług alternatywnych względem usług strażnika dostępu, lecz nie należy go interpretować jako obowiązku użytkownika biznesowego do oferowania swoim użytkownikom końcowym takich alternatywnych usług.
- (44) Praktyka polegająca na nakładaniu na użytkowników biznesowych lub użytkowników końcowych wymogu subskrypcji innej podstawowej usługi platformowej świadczonej przez strażników dostępu, która została wymieniona w decyzji o wskazaniu lub osiągnięciu progi dotyczące aktywnych użytkowników końcowych i użytkowników biznesowych określone w niniejszym rozporządzeniu, lub zarejestrowania się jako użytkownik takiej usługi jako warunek korzystania z podstawowej usługi platformowej, uzyskania dostępu do niej, zapisania się do niej lub zarejestrowania do niej, daje strażnikom dostępu możliwość pozyskiwania nowych użytkowników biznesowych i użytkowników końcowych oraz uzależnienia ich do swoich podstawowych usług platformowych poprzez powiązanie dostępu do jednej podstawowej usługi platformowej dla użytkowników biznesowych z co najmniej rejestracją lub utworzeniem konta w celu otrzymania drugiej podstawowej usługi platformowej. Praktyka taka daje strażnikom dostępu potencjalną przewagę wynikającą z akumulacji danych. Tym samym praktyka ta może stwarzać bariery wejścia i powinna zostać zakazana.
- (45) Warunki, na jakich strażnicy dostępu świadczą internetowe usługi reklamowe na rzecz użytkowników biznesowych, w tym zarówno reklamodawców, jak i wydawców, są często nieprzejrzyste i niejasne. Taka niejasność jest częściowo powiązana z praktykami kilku platform, ale wynika również z ogromnej złożoności współczesnej reklamy programatycznej. Uznaje się, że sektor ten stał się mniej przejrzysty po wprowadzeniu nowych przepisów dotyczących prywatności. W rezultacie reklamodawcy i wydawcy często nie mają informacji lub wiedzy na temat warunków kupowanych internetowych usług reklamowych i mają mniejszą zdolność zmiany przedsiębiorstwa świadczącego internetowe usługi reklamowe. Ponadto koszty internetowych usług reklamowych na takich warunkach są prawdopodobnie wyższe niż w bardziej uczciwym, przejrzystym i kontestowalnym środowisku platform. Te wyższe koszty zostaną przypuszczalnie odzwierciedlone w cenach, które użytkownicy końcowi płacą za wiele codziennych produktów i usług opartych na wykorzystaniu internetowych usług reklamowych. Obowiązki w zakresie przejrzystości powinny zatem obejmować wymóg, aby strażnicy dostępu udzielali reklamodawcom i wydawcom, na rzecz których świadczą internetowe usługi reklamowe, na ich wniosek, nieodpłatnych informacji, które umożliwiają obu stronom zrozumienie ceny płaconej za każdą z poszczególnych internetowych usług reklamowych świadczonych w ramach danego łańcucha wartości reklam.

Informacji tych należy udzielać reklamodawcy, na jego wniosek, na poziomie pojedynczej reklamy w odniesieniu do ceny i opłat pobranych od tego reklamodawcy oraz – z zastrzeżeniem zgody wydawcy będącego właścicielem zasobów, w ramach których reklama jest wyświetlana – do wynagrodzenia otrzymanego przez tego wydawcę wyrażającego zgodę. Udzielanie tych informacji w trybie codziennym zapewni reklamodawcom uzyskanie informacji o wystarczającym poziomie szczegółowości niezbędnym do porównania kosztów korzystania z internetowych usług reklamowych świadczonych przez strażnika dostępu z kosztami korzystania z internetowych usług reklamowych świadczonych przez alternatywne przedsiębiorstwa. W przypadku niewyrażenia przez niektórych wydawców zgody na udostępnienie reklamodawcy odpowiednich informacji, strażnik dostępu powinien udzielać reklamodawcy

informacji dotyczących średniego dziennego wynagrodzenia otrzymywanego przez tych wydawców z tytułu odpowiednich reklam. Ten sam obowiązek i te same zasady udostępniania odpowiednich informacji dotyczących świadczenia internetowych usług reklamowych powinny mieć zastosowanie do wniosków wydawców. Ponieważ strażnicy dostępu mogą stosować różne modele cenowe do świadczenia reklamodawcom i wydawcom internetowych usług reklamowych, na przykład ceny za wyświetlenie, za obejrzenie lub z zastosowaniem innego kryterium, powinni oni również udzielać informacji o metodzie obliczania poszczególnych cen i wynagrodzeń.

- (46) W pewnych okolicznościach strażnik dostępu ma podwójną rolę, będąc przedsiębiorstwem świadczącym podstawowe usługi platformowe, w której to roli świadczy na rzecz swoich użytkowników biznesowych podstawową usługę platformową i ewentualnie inne usługi świadczone wraz z taką usługą lub ją wspierające, a jednocześnie również konkurując lub próbując konkurować z tymi samymi użytkownikami biznesowymi w oferowaniu takich samych lub podobnych usług lub produktów na rzecz tych samych użytkowników końcowych. W tych okolicznościach strażnik dostępu może dzięki swojej podwójnej roli wykorzystywać – do celów oferowanych przez siebie usług lub produktów – dane wygenerowane lub dostarczone przez jego użytkowników biznesowych w ramach aktywności tych użytkowników biznesowych w trakcie korzystania z podstawowych usług platformowych lub usług świadczonych wraz z takimi usługami lub je wspierających. Dane użytkownika biznesowego mogą również obejmować wszelkie dane wygenerowane lub dostarczone w trakcie aktywności jego użytkowników końcowych. Może tak być na przykład wtedy, gdy strażnik dostępu zapewnia użytkownikom biznesowym internetową platformę handlową lub sklep z aplikacjami, a jednocześnie świadczy usługi jako przedsiębiorstwo świadczące internetowe usługi detaliczne lub dostarczające aplikacje. W celu uniemożliwienia strażnikom dostępu czerpania korzyści z ich podwójnej roli, niezbędne jest zapewnienie, aby nie wykorzystywali oni danych zagregowanych lub niezagregowanych, które mogą obejmować dane zanonimizowane i dane osobowe niebędące publicznie dostępne, do świadczenia usług podobnych do usług świadczonych przez ich użytkowników biznesowych. Obowiązek ten powinien mieć zastosowanie do wszystkich jednostek strażnika dostępu, między innymi do jego jednostki organizacyjnej, która konkuruje z użytkownikami biznesowymi podstawowej usługi platformowej.
- (47) Użytkownicy biznesowi mogą również kupować od przedsiębiorstwa świadczącego podstawowe usługi platformowe internetowe usługi reklamowe w celu dostarczania towarów i świadczenia usług na rzecz użytkowników końcowych. W tym przypadku może zdarzyć się, że dane nie są generowane w ramach podstawowej usługi platformowej, lecz są dostarczane przez użytkownika biznesowego na potrzeby takiej usługi lub generowane na podstawie jego działań podejmowanych za pośrednictwem odpowiedniej podstawowej usługi platformowej. W niektórych przypadkach podmiot świadczący taką podstawową usługę platformową zapewniającą reklamę może pełnić podwójną rolę – przedsiębiorstwa świadczącego internetowe usługi reklamowe i przedsiębiorstwa świadczącego usługi konkurujące z usługami użytkownika biznesowego. Wówczas obowiązek, w ramach którego zakazuje się strażnikowi dostępu pełniącemu podwójną rolę wykorzystywania danych użytkowników biznesowych, powinien mieć zastosowanie również w odniesieniu do danych, które przedsiębiorstwa dostarczyły na potrzeby danej podstawowej usługi platformowej do celów internetowych usług reklamowych świadczonych za pośrednictwem tej podstawowej usługi platformowej.
- (48) W odniesieniu do usług przetwarzania w chmurze obowiązek, w ramach którego zakazuje się wykorzystywania danych użytkowników biznesowych, powinien obejmować dane dostarczane lub generowane przez użytkowników biznesowych strażnika dostępu w ramach korzystania przez nich z usługi przetwarzania w chmurze świadczonej przez strażnika dostępu lub poprzez korzystanie z jego sklepu z aplikacjami, który umożliwia użytkownikom końcowym usług przetwarzania w chmurze dostęp do aplikacji. Obowiązek ten nie powinien mieć wpływu na prawo strażnika dostępu do wykorzystywania zagregowanych danych do celów innych usług świadczonych wraz z podstawową usługą platformową strażnika dostępu lub wspierających taką usługę, jak usługi w zakresie analizy danych, z zastrzeżeniem zachowania zgodności z rozporządzeniem (UE) 2016/679 i dyrektywą 2002/58/WE, a także z odpowiednimi obowiązkami dotyczącymi takich usług ustanowionymi w niniejszym rozporządzeniu.
- (49) Strażnik dostępu może stosować różne środki w celu faworyzowania w swoim systemie operacyjnym, wirtualnym asystencie lub przeglądarce internetowej własnych usług lub produktów bądź usług lub produktów osoby trzeciej, ze szkodą dla takich samych lub podobnych usług, które użytkownicy końcowi mogliby otrzymać za pośrednictwem innych osób trzecich. Może tak się zdarzyć na przykład wtedy, gdy pewne aplikacje lub usługi są przez strażnika dostępu preinstalowane. Aby dać użytkownikom końcowym sposobność wyboru, strażnik dostępu nie powinien uniemożliwiać im odinstalowania aplikacji w ich systemie operacyjnym. Strażnik dostępu powinien mieć możliwość ograniczenia takiego odinstalowania wyłącznie w przypadku, gdy takie aplikacje są niezbędne do funkcjonowania systemu operacyjnego lub urządzenia. Strażnik dostępu powinien również umożliwiać użytkownikom końcowym łatwą zmianę domyślnych ustawień systemu operacyjnego, wirtualnego asystenta i przeglądarki internetowej.

towej, gdy te domyślne ustawienia faworyzują jego własne aplikacje i usługi. Obejmuje to wyświetlenie ekranu wyboru w momencie korzystania przez użytkownika po raz pierwszy z wyszukiwarki internetowej, wirtualnego asystenta lub przeglądarki internetowej strażnika dostępu wymienionych w decyzji o wskazaniu, pozwalającego użytkownikom końcowym wybrać alternatywną usługę domyślną, w przypadku gdy system operacyjny strażnika dostępu kieruje ich do tej wyszukiwarki internetowej, tego wirtualnego asystenta lub tej przeglądarki internetowej i w przypadku gdy wirtualny asystent lub przeglądarka internetowa strażnika dostępu kierują użytkownika do wyszukiwarki internetowej wymienionej w decyzji o wskazaniu.

- (50) Zasady, które strażnik dostępu ustala w odniesieniu do dystrybucji aplikacji, mogą w niektórych okolicznościach ograniczać użytkownikom końcowym możliwość instalowania aplikacji lub sklepów z aplikacjami oferowanych przez osoby trzecie na sprzęcie lub w systemach operacyjnych tego strażnika dostępu i skutecznego korzystania z takich aplikacji lub sklepów oraz ograniczać użytkownikom końcowym możliwość dostępu do takich aplikacji lub sklepów z aplikacjami poza podstawową usługą platformową tego strażnika dostępu. Takie ograniczenia mogą ograniczać deweloperom aplikacji możliwość korzystania z alternatywnych kanałów dystrybucji oraz ograniczać użytkownikom końcowym swobodę wyboru spośród różnych aplikacji z różnych kanałów dystrybucji, powinny zatem zostać zakazane jako nieuczciwe i mogące osłabiać kontestowalność podstawowych usług platformowych. W celu zapewnienia kontestowalności strażnik dostępu powinien ponadto umożliwić aplikacjom lub sklepom z aplikacjami oferowanym przez osoby trzecie skłanianie użytkowników końcowych do decydowania, czy ta usługa powinna stać się domyślną, i powinien umożliwić przeprowadzenie odnośnej zmiany w łatwy sposób.

W celu zapewnienia, aby aplikacje lub sklepy z aplikacjami oferowane przez osoby trzecie nie zagrażały integralności sprzętu lub systemu operacyjnego dostarczanego przez strażnika dostępu, dany strażnik dostępu powinien mieć możliwość wdrożenia proporcjonalnych środków technicznych lub umownych służących osiągnięciu tego celu, o ile wykaże, że takie środki są niezbędne i uzasadnione oraz że nie istnieją mniej restrykcyjne sposoby pozwalające zabezpieczyć integralność tego sprzętu lub systemu operacyjnego. Integralność sprzętu lub systemu operacyjnego powinna obejmować wszelkie opcje projektowe, których wdrożenie i utrzymanie jest niezbędne w celu ochrony sprzętu i systemu operacyjnego przed nieuprawnionym dostępem poprzez zapewnienie, by określone dla danego sprzętu lub systemu operacyjnego kontrole bezpieczeństwa nie były zagrożone. Ponadto w celu zapewnienia, by aplikacje lub sklepy z aplikacjami oferowane przez osoby trzecie nie zagrażały bezpieczeństwu użytkowników końcowych, strażnik dostępu powinien mieć możliwość wdrożenia bezwzględnie koniecznych i proporcjonalnych środków i ustawień, innych niż ustawienia domyślne, umożliwiających użytkownikom końcowym skuteczną ochronę bezpieczeństwa w odniesieniu do aplikacji lub sklepów z aplikacjami oferowanych przez osoby trzecie, o ile strażnik dostępu wykaże, że takie środki i ustawienia są bezwzględnie konieczne i proporcjonalne oraz że nie istnieją mniej restrykcyjne środki pozwalające osiągnąć ten cel. Należy uniemożliwić strażnikowi dostępu wdrażanie takich środków poprzez ustawienia domyślne lub preinstalację.

- (51) Strażnicy dostępu są często zintegrowani pionowo i oferują użytkownikom końcowym produkty lub usługi za pośrednictwem własnych podstawowych usług platformowych lub za pośrednictwem użytkownika biznesowego, nad którym sprawują kontrolę, co niejednokrotnie prowadzi do konfliktu interesów. Przykładem jest sytuacja, w której strażnik dostępu świadczy własne usługi pośrednictwa internetowego za pośrednictwem wyszukiwarki internetowej. Gdy strażnicy dostępu oferują te produkty lub usługi w ramach podstawowej usługi platformowej, mogą zarezerwować lepszą pozycję pod względem plasowania i związanego z nim indeksowania i badania (crawlingu) dla własnej oferty niż dla produktów lub usług osób trzecich również działających w ramach tej podstawowej usługi platformowej. Może się tak wydarzyć na przykład w przypadku produktów lub usług, w tym innych podstawowych usług platformowych, które są plasowane w wynikach prezentowanych przez wyszukiwarki internetowe lub które są częściowo lub w całości osadzone w wynikach wyszukiwarek internetowych, tj. grupach wyników dotyczących konkretnych tematów, wyświetlanych wraz z wynikami wyszukiwarek internetowych, które są traktowane lub wykorzystywane przez niektórych użytkowników końcowych jako usługa odrębna lub dodatkowa w stosunku do wyszukiwarki internetowej.

Inne przypadki dotyczą aplikacji, których dystrybucja odbywa się za pośrednictwem sklepów z aplikacjami, lub wideo, których dystrybucja odbywa się poprzez platformy udostępniania wideo, lub produktów lub usług, które są widoczne i wyświetlane w kanale aktualności internetowej serwisu społecznościowego, lub też produktów lub usług plasowanych w wynikach wyszukiwania lub wyświetlanych na internetowej platformie handlowej, lub produktów lub usług, które są oferowane za pośrednictwem wirtualnego asystenta. Takie rezerwowanie przez strażnika dostępu lepszej pozycji dla własnej oferty może mieć miejsce, nawet zanim nastąpi plasowanie na skutek dokonania zapytania, na przykład w toku badania (crawlingu) i indeksowania. Na przykład strażnik dostępu może faworyzować

własną treść względem treści osób trzecich już podczas badania (crawlingu), jako procesu wykrywania, w ramach którego znajdują się nowe i zaktualizowane treści, a także podczas indeksowania, które wiąże się z przechowywaniem i porządkowaniem treści znalezionych podczas badania (crawlingu). W tych okolicznościach strażnik dostępu pełni podwójną rolę – pośrednika dla przedsiębiorstw będących osobami trzecimi oraz przedsiębiorstwa bezpośrednio oferującego produkty lub usługi. W konsekwencji tacy strażnicy dostępu mają zdolność bezpośredniego osłabiania kontestowalności tych produktów lub usług w ramach tych podstawowych usług platformowych, ze szkodą dla użytkowników biznesowych, którzy nie są kontrolowani przez danego strażnika dostępu.

- (52) W takich sytuacjach strażnik dostępu nie powinien dopuszczać się, za pomocą środków prawnych, handlowych lub technicznych, żadnych form różnicowanego lub preferencyjnego traktowania w plasowaniu w ramach podstawowej usługi platformowej i związanych z nim indeksowaniu i badaniu (crawlingu) na korzyść produktów lub usług, które oferuje sam lub za pośrednictwem kontrolowanego przez siebie użytkownika biznesowego. W celu zapewnienia skuteczności tego obowiązku również warunki, które mają zastosowanie do takiego plasowania, powinny być ogólnie uczciwe i przejrzyste. Plasowanie powinno w tym kontekście obejmować wszystkie formy określonej widoczności, w tym wyświetlanie, przedstawianie rankingu, linkowanie lub wyniki głosowe i powinno także obejmować wszystkie przypadki, w których podstawowa usługa platformowa przedstawia lub przekazuje użytkownikowi końcowemu tylko jeden wynik. W celu zapewnienia, aby obowiązek ten był skuteczny i nie mógł być obchodzony, powinien on mieć zastosowanie również do każdego środka, który ma skutek równoważny ze różnicowanym lub preferencyjnym traktowaniem w plasowaniu. Wytyczne przyjęte na podstawie art. 5 rozporządzenia (UE) 2019/1150 powinny również ułatwiać wdrażanie i egzekwowanie tego obowiązku.
- (53) Strażnicy dostępu nie powinni ograniczać ani uniemożliwiać swobody wyboru użytkownikom końcowym przez uniemożliwianie im za pośrednictwem środków technicznych lub w inny sposób zmiany aplikacji i usług lub subskrybowania innych aplikacji i usług. Umożliwiłyby to większej liczbie przedsiębiorstw oferowanie swoich usług, a tym samym ostatecznie zapewniłyby użytkownikowi końcowemu większy wybór. Strażnicy dostępu powinni zapewniać swobodę wyboru niezależnie od tego, czy są producentami jakiegokolwiek sprzętu zapewniającego dostęp do takich aplikacji lub usług, oraz nie powinni stwarzać sztucznych barier technicznych lub innych sprawiających, że zmiana aplikacji lub usługi staje się niemożliwa lub nieskuteczna. Samego zaoferowania danego produktu lub danej usługi konsumentom, w tym poprzez preinstalację, a także przedstawiania ulepszonej oferty dla użytkowników końcowych, obejmującej między innymi niższą cenę lub wyższą jakość, nie należy uznawać za stanowiące zakazaną barierę utrudniającą zmianę.
- (54) Strażnicy dostępu mogą utrudniać użytkownikom końcowym możliwość dostępu do treści i usług internetowych, w tym aplikacji. W związku z tym należy ustanowić przepisy w celu zapewnienia, aby prawa użytkowników końcowych do dostępu do otwartego internetu nie były zagrożone przez praktyki strażników dostępu. Strażnicy dostępu mogą również technicznie ograniczać użytkownikom końcowym możliwość skutecznej zmiany przedsiębiorstwa świadczącego usługę dostępu do internetu, w szczególności sprawując kontrolę nad sprzętem lub systemami operacyjnymi. Zakłóca to równe warunki działania w zakresie usług dostępu do internetu i ostatecznie szkodzi użytkownikom końcowym. Należy w związku z tym zapewnić, aby strażnicy dostępu nie ograniczali użytkownikom końcowym w sposób nienależyty swobody wyboru przedsiębiorstwa świadczącego usługę dostępu do internetu.
- (55) Strażnik dostępu może świadczyć usługi lub dostarczać sprzęt, taki jak urządzenia ubieralne, które w celu zaoferowania określonych funkcjonalności użytkownikom końcowym uzyskują dostęp do funkcji sprzętu lub oprogramowania danego urządzenia, do którego uzyskuje się dostęp lub które jest kontrolowane za pośrednictwem systemu operacyjnego lub wirtualnego asystenta. W takim przypadku konkurujący dostawcy usług lub sprzętu, tacy jak dostawcy urządzeń ubieralnych, aby móc dostarczyć konkurencyjną ofertę użytkownikom końcowym, potrzebują również skutecznej interoperacyjności z tymi samymi funkcjami sprzętu lub oprogramowania i również skutecznego dostępu do tych funkcji na potrzeby interoperacyjności.
- (56) Strażnicy dostępu mogą również pełnić podwójną rolę deweloperów systemów operacyjnych i producentów urządzeń, w tym wszelkich funkcjonalności technicznych, w które takie urządzenie może być wyposażone. Na przykład strażnik dostępu, który jest producentem urządzenia, może ograniczyć dostęp do niektórych funkcjonalności w tym urządzeniu, takich jak technologia komunikacji zbliżeniowej, zabezpieczenia i bezpieczne procesory, mechanizmy uwierzytelnienia i oprogramowanie używane do obsługi tych technologii, które mogą być wymagane do skutecznego świadczenia przez strażnika dostępu usługi świadczonej wraz z podstawową usługą platformową lub wspierającą taką usługę, a także przez potencjalne przedsiębiorstwo świadczące taką usługę jako osoba trzecia.

- (57) Jeżeli podwójne role są wykorzystywane w sposób uniemożliwiający alternatywnym dostawcom usług lub sprzętu dostęp na równych warunkach do tego samego systemu operacyjnego, funkcji sprzętu lub oprogramowania, do których strażnik dostępu ma dostęp lub które wykorzystuje, by świadczyć własne uzupełniające lub wspierające usługi lub dostarczać własny uzupełniający lub wspierający sprzęt, może to znacząco osłabić innowacyjność tych alternatywnych dostawców, a także ograniczyć wybór użytkownikom końcowym. W związku z tym na strażnikach dostępu powinien spoczywać wymóg zapewnienia nieodpłatnie skutecznej interoperacyjności z tym samym systemem operacyjnym, funkcjami sprzętu lub oprogramowania i dostępu do nich na potrzeby interoperacyjności, które to system i funkcje są dostępne dla nich lub używane przez nich do świadczenia własnych uzupełniających i wspierających usług lub dostarczania własnego uzupełniającego lub wspierającego sprzętu. Takiego dostępu mogą również wymagać aplikacje związane z odpowiednimi usługami świadczonymi wraz z podstawową usługą platformową lub wspierającymi takie usługi – w celu skutecznego rozwijania i dostarczania funkcjonalności interoperacyjnych z funkcjonalnościami dostarczonymi przez strażników dostępu. Celem obowiązków jest umożliwienie konkurującym osobom trzecim łączenia się za pośrednictwem interfejsów lub podobnych rozwiązań z odpowiednimi funkcjami tak skutecznie, jak ma to miejsce w przypadku własnych usług lub sprzętu strażnika dostępu.
- (58) Warunki, na jakich strażnicy dostępu świadczą internetowe usługi reklamowe na rzecz użytkowników biznesowych, w tym zarówno reklamodawców, jak i wydawców, są często nieprzejrzyste i niejasne. W rezultacie reklamodawcy i wydawcy często nie mają informacji na temat skutku wywołanego przez daną reklamę. Aby jeszcze bardziej zwiększyć uczciwość, przejrzystość i kontestowalność internetowych usług reklamowych wymienionych w decyzji o wskazaniu, jak również tych usług, które są w pełni zintegrowane z innymi podstawowymi usługami platformowymi tego samego przedsiębiorstwa, strażnicy dostępu powinni zapewniać reklamodawcom i wydawcom oraz upoważnionym przez reklamodawców i wydawców osobom trzecim, na ich wniosek, nieodpłatny dostęp do stosowanych przez siebie narzędzi pomiaru wyników oraz do danych, w tym danych zagregowanych i niezagregowanych, które są niezbędne reklamodawcom, upoważnionym osobom trzecim, takim jak agencje reklamowe działające w imieniu przedsiębiorstwa umieszczającego reklamę, a także wydawcom do przeprowadzenia samodzielnie niezależnej weryfikacji świadczenia odpowiednich internetowych usług reklamowych.
- (59) Strażnicy dostępu czerpią korzyści z dostępu do dużych ilości danych, które zbierają podczas świadczenia podstawowych usług platformowych, a także innych usług cyfrowych. W celu zapewnienia, aby strażnicy dostępu nie osłabiali kontestowalności podstawowych usług platformowych lub istniejącego w ramach dynamicznego sektora cyfrowego potencjału w zakresie innowacji przez ograniczanie możliwości zmiany lub korzystania z wielu platform (*multi-homing*), należy udzielić użytkownikom końcowym, a także upoważnionym przez nich osobom trzecim skutecznego i natychmiastowego dostępu do danych, które dostarczyli lub które zostały wygenerowane w toku ich działalności w ramach odpowiednich podstawowych usług platformowych strażników dostępu. Dane powinny być otrzymywane w formacie, który umożliwia natychmiastowe i skuteczne uzyskanie dostępu do nich i ich wykorzystanie przez użytkownika końcowego lub odpowiednią osobę trzecią, upoważnioną przez użytkownika końcowego, do której dane są przenoszone. Strażnicy dostępu powinni również zapewnić za pomocą odpowiednich i wysokiej jakości środków technicznych, takich jak interfejsy programowania aplikacyjnego, możliwość ciągłego, przebiegającego w czasie rzeczywistym swobodnego przenoszenia danych przez użytkowników końcowych lub osoby trzecie upoważnione przez użytkowników końcowych. Powinno to mieć zastosowanie również do innych danych na różnych poziomach zagregowania niezbędnych do tego, by skutecznie umożliwić takie przenoszenie. Dla uniknięcia wątpliwości spoczywający na strażniku dostępu obowiązek zapewnienia skutecznego przenoszenia danych wynikający z niniejszego rozporządzenia stanowi uzupełnienie prawa do przenoszenia danych ustanowionego w rozporządzeniu (UE) 2016/679. Ułatwienie dokonywania zmiany lub korzystania z wielu platform (*multi-homing*) powinno z kolei prowadzić do zwiększenia wyboru dla użytkowników końcowych i stanowi zachętę dla strażników dostępu i użytkowników biznesowych do innowacji.
- (60) Użytkownicy biznesowi, którzy korzystają z podstawowych usług platformowych świadczonych przez strażników dostępu, i użytkownicy końcowi takich użytkowników biznesowych dostarczają i generują ogromne ilości danych. W celu zapewnienia, aby użytkownicy biznesowi mieli dostęp do odpowiednich danych wygenerowanych w ten sposób, strażnik dostępu powinien – na ich wniosek – udzielić skutecznego i nieodpłatnego dostępu do takich danych. Takiego dostępu należy również udzielić osobom trzecim, z którymi użytkownik biznesowy zawarł umowę i które działają jako podmioty przetwarzające te dane na rzecz użytkownika biznesowego. Dostęp ten powinien obejmować dostęp do danych dostarczanych lub generowanych przez tych samych użytkowników biznesowych i tych samych użytkowników końcowych tych użytkowników biznesowych w ramach innych usług świadczonych przez tego samego strażnika dostępu, w tym usług świadczonych wraz z podstawowymi usługami platformowymi lub wspierających takie usługi, o ile dane takie są nierozdzielnie związane z konkretnym wnioskiem. W tym celu strażnik dostępu nie powinien stosować żadnych ograniczeń umownych ani innych w celu uniemożliwiania użytkownikom biznesowym dostępu do odpowiednich danych oraz powinien umożliwiać użytkownikom biznesowym uzyskanie zgody ich użytkowników końcowych na udzielenie dostępu do takich danych i ich wyszukiwanie, gdy taka zgoda jest wymagana zgodnie z rozporządzeniem (UE) 2016/679 i dyrektywą 2002/58/WE. Strażnicy dostępu powinni również zapewniać stały dostęp do takich danych w czasie rzeczywistym za pomocą odpowiednich środków technicznych, na przykład poprzez wdrożenie wysokiej jakości interfejsów programowania aplikacyjnego lub zintegrowanych narzędzi dla drobnych użytkowników biznesowych.

- (61) Wartość wyszukiwarek internetowych dla ich użytkowników biznesowych i użytkowników końcowych rośnie wraz ze wzrostem całkowitej liczby takich użytkowników. Przedsiębiorstwa będące dostawcami wyszukiwarek internetowych zbierają i przechowują zagregowane zbiory danych zawierające informacje na temat tego, czego dotyczyły wyszukiwania przeprowadzone przez użytkowników i jaka była ich interakcja z wynikami, które im dostarczono. Przedsiębiorstwa będące dostawcami wyszukiwarek internetowych zbierają te dane z wyszukiwań przeprowadzanych w ramach ich własnej wyszukiwarki internetowej oraz, w stosownych przypadkach, z wyszukiwań przeprowadzanych na platformach ich partnerów handlowych niższego szczebla. Dostęp strażników dostępu do takich danych na temat plasowania, zapytań, kliknięć i wyświetleń stanowi ważną barierę wejścia i rozszerzania działalności, która osłabia kontestowalność wyszukiwarek internetowych. W związku z tym na strażnikach dostępu powinien spoczywać wymóg udzielania – na uczciwych, rozsądnych i niedyskryminujących warunkach – dostępu do tych danych na temat plasowania, zapytań, kliknięć i wyświetleń związanych z nieodpłatnym i płatnym wyszukiwaniem, wygenerowanych przez konsumentów w ramach wyszukiwarek internetowych, innym przedsiębiorstwom świadczącym takie usługi, tak aby te przedsiębiorstwa będące osobami trzecimi mogły optymalizować swoje usługi i konkurować z odpowiednimi podstawowymi usługami platformowymi. Taki dostęp powinny również uzyskać osoby trzecie, z którymi dostawca wyszukiwarki internetowej zawarł umowę i które działają jako podmioty przetwarzające te dane na rzecz danej wyszukiwarki internetowej. Przy udzielaniu dostępu do danych na temat wyszukiwania strażnik dostępu powinien zapewnić ochronę danych osobowych użytkowników końcowych, w tym przed zagrożeniami związanymi z deanonimizacją, za pomocą odpowiednich środków, takich jak anonimizacja takich danych osobowych, bez znacznego obniżania jakości lub przydatności danych. Odpowiednie dane są zanonimizowane, gdy dane osobowe są nieodwracalnie zmienione w taki sposób, że informacje nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, lub gdy dane osobowe zostały zanonimizowane w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można ich zidentyfikować.
- (62) W odniesieniu do wymienionych w decyzji o wskazaniu sklepów z aplikacjami, wyszukiwarek internetowych i internetowych serwisów społecznościowych strażnik dostępu powinien publikować ogólne warunki dostępu, które powinny być uczciwe, rozsądne i niedyskryminujące, i stosować takie warunki. Te ogólne warunki powinny przewidywać unijny alternatywny mechanizm rozstrzygania sporów, który będzie łatwo dostępny, bezstronny, niezależny i bezpłatny dla użytkownika biznesowego, z zastrzeżeniem kosztów własnych użytkownika biznesowego i bez uszczerbku dla proporcjonalnych środków mających na celu zapobieganie nadużywaniu mechanizmu rozstrzygania sporów przez użytkowników biznesowych. Mechanizm rozstrzygania sporów powinien pozostawać bez uszczerbku dla prawa użytkowników biznesowych do dochodzenia roszczeń przed organami sądowymi zgodnie z prawem Unii i prawem krajowym. W szczególności strażnicy dostępu, którzy udzielają dostępu do sklepów z aplikacjami, są ważnym punktem dostępu dla użytkowników biznesowych, którzy chcą dotrzeć do użytkowników końcowych. W świetle braku równowagi w zakresie siły przetargowej pomiędzy tymi strażnikami dostępu a korzystającymi z ich sklepów z aplikacjami użytkownikami biznesowymi należy zakazać tym strażnikom dostępu stosowania warunków ogólnych, w tym warunków ustalania cen, które byłyby nieuczciwe lub prowadziłyby do nieuzasadnionego różnicowania.

Ustalanie cen lub inne ogólne warunki dostępu powinny być uznawane za nieuczciwe, jeżeli prowadzą do braku równowagi między prawami i obowiązkami nakładanymi na użytkowników biznesowych lub dają strażnikowi dostępu przewagę, która jest nieproporcjonalna do usługi świadczonej przez niego na rzecz użytkowników biznesowych, lub jeżeli sprawiają, że użytkownicy biznesowi, którzy świadczą takie same lub podobne usługi jak strażnik dostępu, znajdują się w mniej korzystnej sytuacji. Następujące wartości odniesienia mogą służyć jako kryteria określania uczciwości ogólnych warunków dostępu: ceny lub warunki nakładane w odniesieniu do takich samych lub podobnych usług przez innych dostawców sklepów z aplikacjami; ceny lub warunki nakładane przez dostawcę sklepu z aplikacjami w odniesieniu do innych powiązanych lub podobnych usług lub w stosunku do innych rodzajów użytkowników końcowych; ceny lub warunki nakładane przez dostawcę sklepu z aplikacjami w odniesieniu do takiej samej usługi w innych regionach geograficznych; ceny lub warunki nakładane przez dostawcę sklepu z aplikacjami w odniesieniu do takiej samej usługi, którą strażnik dostępu sam świadczy. Obowiązek ten nie powinien prowadzić do ustanowienia prawa dostępu i powinien pozostawać bez uszczerbku dla zdolności przyjmowania przez dostawców sklepów z aplikacjami, wyszukiwarek internetowych i internetowych serwisów społecznościowych wymaganej odpowiedzialności w ramach zwalczania nielegalnych i niechcianych treści, jak określono w rozporządzeniu w sprawie jednolitego rynku usług cyfrowych.

- (63) Strażnicy dostępu mogą utrudniać użytkownikom biznesowym i użytkownikom końcowym możliwość rezygnacji z subskrypcji podstawowej usługi platformowej, w przypadku której dokonali oni wcześniej subskrypcji. Należy zatem ustanowić przepisy, aby uniknąć sytuacji, w której strażnicy dostępu osłabiają prawa użytkowników biznesowych i użytkowników końcowych do swobodnego wyboru, z jakiej podstawowej usługi platformowej korzystają. Aby zagwarantować użytkownikom biznesowym i użytkownikom końcowym swobodny wybór, należy zakazać strażnikom dostępu niepotrzebnego utrudniania lub komplikowania użytkownikom biznesowym lub użytkownikom końcowym rezygnacji z subskrypcji podstawowej usługi platformowej. Zamknięcie konta lub rezygnacja



z subskrypcji nie powinny być bardziej skomplikowane niż założenie konta lub subskrybowanie takiej samej usługi. Rozwiązując umowy z użytkownikami końcowymi lub użytkownikami biznesowymi, strażnicy dostępu nie powinni żądać dodatkowych opłat. Strażnicy dostępu powinni zapewnić, aby warunki rozwiązywania umów były zawsze proporcjonalne i mogły być spełnione przez użytkowników końcowych bez zbędnych trudności, na przykład w odniesieniu do przyczyn rozwiązania umowy, okresu wypowiedzenia lub formy takiego rozwiązania. Pozostaje to bez uszczerbku dla przepisów krajowych mających zastosowanie zgodnie z prawem Unii ustanawiającym prawa i obowiązki dotyczące warunków rezygnacji przez użytkowników końcowych z podstawowych usług platformowych.

- (64) Brak interoperacyjności pozwala strażnikom dostępu, którzy świadczą usługi łączności interpersonalnej niewykorzystujące numerów, wykorzystywać silne efekty sieciowe, co przyczynia się do osłabienia kontestowalności. Ponadto, bez względu na to, czy użytkownicy końcowi korzystają z wielu platform („multi-homing”), strażnicy dostępu często świadczą usługi łączności interpersonalnej niewykorzystujące numerów jako element swojego ekosystemu platform, a to dodatkowo zwiększa bariery wejścia dla alternatywnych dostawców takich usług i podnosi ponoszone przez użytkowników końcowych koszty zmiany. Bez uszczerbku dla dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 <sup>(14)</sup>, a w szczególności warunków i procedur określonych w jej art. 61, strażnicy dostępu powinni zatem zapewnić osobom trzecim będącym dostawcami usług łączności interpersonalnej niewykorzystujących numerów, bezpłatnie i na wniosek, interoperacyjność z określonymi podstawowymi funkcjonalnościami usług łączności interpersonalnej niewykorzystujących numerów, które to usługi świadczą swoim użytkownikom końcowym.

Strażnicy dostępu powinni zapewniać interoperacyjność osobom trzecim będącym dostawcami usług łączności interpersonalnej niewykorzystujących numerów, którzy oferują lub zamierzają oferować swoje usługi łączności interpersonalnej niewykorzystujące numerów użytkownikom końcowym i użytkownikom biznesowym w Unii. Aby ułatwić praktyczne wdrożenie takiej interoperacyjności, na odpowiednim strażniku dostępu powinien spoczywać wymóg opublikowania oferty ramowej określającej szczegółowe informacje techniczne oraz ogólne warunki interoperacyjności ze świadczonymi przez niego usługami łączności interpersonalnej niewykorzystującymi numerów. W stosownych przypadkach Komisja powinna mieć możliwość skonsultowania się z Organem Europejskich Regulatorów Łączności Elektronicznej w celu ustalenia, czy szczegółowe informacje techniczne oraz ogólne warunki opublikowane w ofercie ramowej, którą strażnik dostępu zamierza realizować lub już realizuje, zapewniają wypełnienie tego obowiązku.

We wszystkich przypadkach strażnik dostępu i dostawca występujący z wnioskiem powinni zapewnić, by interoperacyjność nie stanowiła zagrożenia dla wysokiego poziomu bezpieczeństwa i ochrony danych zgodnie z ich obowiązkami ustanowionymi w niniejszym rozporządzeniu i w mającym zastosowanie prawie Unii, w szczególności rozporządzeniu (UE) 2016/679 i dyrektywie 2002/58/WE. Obowiązek dotyczący interoperacyjności powinien pozostawać bez uszczerbku dla informacji i możliwości wyboru udostępnianych – na podstawie niniejszego rozporządzenia i innych przepisów prawa Unii, w szczególności rozporządzenia (UE) 2016/679 – końcowym użytkownikom usług łączności interpersonalnej niewykorzystujących numerów, świadczonych przez strażnika dostępu i dostawcę występującego z wnioskiem.

- (65) W celu zapewnienia skuteczności obowiązków ustanowionych w niniejszym rozporządzeniu, a jednocześnie dopilnowania, aby były one ograniczone do tego, co jest konieczne do zapewnienia kontestowalności i zwalczania szkodliwych skutków nieuczciwych praktyk strażników dostępu, ważne jest jasne sformułowanie i określenie tych obowiązków, tak aby strażnik dostępu mógł wypełnić je w pełni, z pełnym poszanowaniem mających zastosowanie przepisów, w szczególności rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, oraz przepisów w zakresie ochrony konsumentów, cyberbezpieczeństwa, bezpieczeństwa produktów i wymogów dostępności, w tym dyrektyw Parlamentu Europejskiego i Rady (UE) 2019/882 i (UE) 2016/2102 <sup>(15)</sup>. Strażnicy dostępu powinni zapewniać zgodność z niniejszym rozporządzeniem już na etapie projektowania. Niezbędne środki powinny zatem zostać w jak największym stopniu włączone do projektu technologicznego stosowanego przez strażników dostępu.

<sup>(14)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.U. L 321 z 17.12.2018, s. 36).

<sup>(15)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.U. L 327 z 2.12.2016, s. 1).

W niektórych przypadkach może okazać się właściwe, aby Komisja, po przeprowadzeniu dialogu z danym strażnikiem dostępu oraz po umożliwieniu osobom trzecim zgłoszenia uwag, doprecyzowała niektóre środki, które dany strażnik dostępu powinien zastosować w celu skutecznego wypełnienia obowiązków, które mogą podlegać doprecyzowaniu, lub – w przypadku obchodzenia obowiązków – wszystkich obowiązków. W szczególności takie doprecyzowanie powinno być możliwe w przypadku, gdy występowanie wariantów usług w ramach jednej kategorii podstawowych usług platformowych może mieć wpływ na wykonywanie obowiązku, który może podlegać doprecyzowaniu. W tym celu należy zapewnić strażnikowi dostępu możliwość zwrócenia się do Komisji o wszczęcie postępowania w celu doprecyzowania niektórych środków, które dany strażnik dostępu powinien zastosować w celu skutecznego wypełnienia tych obowiązków.

Komisja powinna mieć swobodę decydowania, czy i kiedy należy dokonać takiego doprecyzowania, przy poszanowaniu zasad równego traktowania, proporcjonalności i dobrej administracji. W związku z tym Komisja powinna przedstawić główne powody będące podstawą dokonanej oceny, w tym dotyczące priorytetów w zakresie egzekwowania. Postępowanie to nie powinno być wykorzystywane w celu podważania skuteczności niniejszego rozporządzenia. Ponadto postępowanie to pozostaje bez uszczerbku dla uprawnień Komisji do przyjęcia decyzji stwierdzającej niewypełnianie przez strażnika dostępu któregośkolwiek z obowiązków ustanowionych w niniejszym rozporządzeniu, w tym możliwości nakładania grzywien lub okresowych kar pieniężnych. Komisja powinna mieć możliwość wznowienia postępowania, również w przypadku gdy doprecyzowane środki okażą się nieskuteczne. Wznowienie ze względu na nieskuteczność dokonanej w drodze decyzji doprecyzowania powinno umożliwić Komisji perspektywę zmiany tego doprecyzowania. Komisja powinna również mieć możliwość określenia rozsądnego okresu, w którym można wznowić postępowanie, jeżeli doprecyzowane środki okażą się nieskuteczne.

- (66) Strażnikom dostępu należy również zapewnić, jako dodatkowy element służący zapewnieniu proporcjonalności, możliwość wystąpienia o zawieszenie określonego obowiązku – w zakresie, w jakim będzie to konieczne – z uwagi na wystąpienie wyjątkowych okoliczności pozostających poza kontrolą strażnika dostępu, takich jak nieprzewidziany wstrząs wywołany czynnikami zewnętrznymi, który tymczasowo wyeliminował znaczną część popytu użytkowników końcowych na odpowiednią podstawową usługę platformową, jeżeli strażnik dostępu będzie w stanie wykazać, że wypełnianie określonego obowiązku zagraża rentowności działalności prowadzonej przez niego w Unii. Komisja powinna określić wyjątkowe okoliczności uzasadniające zawieszenie i regularnie dokonywać ich przeglądu, aby ocenić, czy nadal zachodzą warunki przyznania zawieszenia.
- (67) W wyjątkowych okolicznościach, uzasadnionych wyłącznie względami zdrowia publicznego lub bezpieczeństwa publicznego ustanowionymi w prawie Unii i orzecznictwie Trybunału Sprawiedliwości, Komisja powinna mieć możliwość zdecydowania, że określony obowiązek nie ma zastosowania do danej podstawowej usługi platformowej. Jeżeli taki interes publiczny doznaje uszczerbku, może to świadczyć o tym, że koszt wyegzekwowania danego obowiązku dla całego społeczeństwa jest w określonym wyjątkowym przypadku zbyt wysoki, a zatem nieproporcjonalny. W stosownych przypadkach Komisja powinna mieć możliwość ułatwienia wypełniania obowiązków poprzez dokonanie oceny tego, czy istnieje uzasadnienie dla wprowadzenia ograniczonego i należyście uzasadnionego zawieszenia lub zwolnienia. Powinno to zapewnić proporcjonalność obowiązków ustanowionych w niniejszym rozporządzeniu, nie niwecząc oczekiwanego wpływu *ex ante* na uczciwość i kontestowalność. W przypadku przyznania takiego zwolnienia Komisja powinna dokonywać przeglądu swojej decyzji co rok.
- (68) W terminie wyznaczonym na wypełnienie obowiązków wynikających z niniejszego rozporządzenia strażnicy dostępu powinni w ramach obowiązkowej sprawozdawczości poinformować Komisję o środkach, które zamierzają wdrożyć lub wdrożyli w celu zapewnienia skutecznego wypełniania tych obowiązków, w tym o środkach służących zapewnieniu zgodności z rozporządzeniem (UE) 2016/679, w zakresie, w jakim są one istotne dla wypełniania obowiązków ustanowionych w niniejszym rozporządzeniu, co powinno umożliwić Komisji wykonywanie jej zadań wynikających z niniejszego rozporządzenia. Ponadto należy udostępnić publicznie jasne i zrozumiałe, jawne streszczenie takich informacji, przy jednoczesnym uwzględnieniu uzasadnionego interesu strażników dostępu w zakresie ochrony ich tajemnic handlowych i innych informacji poufnych. To jawne udostępnienie powinno umożliwić osobom trzecim ocenę, czy strażnicy dostępu wypełniają obowiązki ustanowione w niniejszym rozporządzeniu. Taka sprawozdawczość powinna pozostawać bez uszczerbku dla działań w zakresie egzekwowania podejmowanych przez Komisję w dowolnym momencie po dokonaniu tej sprawozdawczości. Komisja powinna udostępniać w internecie link do jawnego streszczenia tego sprawozdania, a także wszelkie inne informacje publiczne na podstawie obowiązków informacyjnych wynikających z niniejszego rozporządzenia, aby zapewnić dostępność takich informacji w sposób użyteczny i kompleksowy, w szczególności dla małych i średnich przedsiębiorstw (MŚP).

- (69) Obowiązki strażników dostępu powinny być aktualizowane wyłącznie po dokładnym zbadaniu charakteru i wpływu konkretnych praktyk, które mogły zostać niedawno zidentyfikowane – w następstwie dogłębnego badania – jako nieuczciwe lub ograniczające kontestowalność w taki sam sposób co nieuczciwe praktyki określone w niniejszym rozporządzeniu, które potencjalnie nie zostały uwzględnione w zakresie obecnego zestawu obowiązków. Komisja powinna mieć możliwość przeprowadzenia badania w celu ustalenia, czy istniejące obowiązki należy zaktualizować, z własnej inicjatywy albo na uzasadniony wniosek co najmniej trzech państw członkowskich. Przedstawiając takie uzasadnione wnioski, państwa członkowskie powinny mieć możliwość uwzględnienia informacji na temat nowo wprowadzonych ofert produktów, usług, oprogramowania lub funkcji, które budzą obawy co do kontestowalności lub uczciwości, niezależnie od tego, czy są one wdrażane w ramach istniejących podstawowych usług platformowych, czy też w inny sposób. W przypadku gdy w wyniku badania rynku Komisja uzna za konieczne zmodyfikowanie istotnych elementów niniejszego rozporządzenia, na przykład poprzez zamieszczenie nowych obowiązków, które dotyczą innych kwestii dotyczących kontestowalności lub uczciwości, ujętych w niniejszym rozporządzeniu, Komisja powinna przedstawić wniosek w sprawie zmiany niniejszego rozporządzenia.
- (70) Ze względu na znaczącą siłę gospodarczą strażników dostępu ważne jest, aby obowiązki były stosowane skutecznie i nie były obchodzone. Aby możliwe było osiągnięcie tego celu, przedmiotowe przepisy powinny mieć zastosowanie do wszelkich praktyk strażnika dostępu, niezależnie od ich formy i niezależnie od tego, czy mają one charakter umowny, handlowy, techniczny czy inny, o ile dana praktyka odpowiada rodzajowi praktyki, którego dotyczy jeden z obowiązków ustanowionych w niniejszym rozporządzeniu. Strażnicy dostępu nie powinni dopuszczać się zachowań, które mogłyby podważyć skuteczność zakazów i obowiązków ustanowionych w niniejszym rozporządzeniu. Takim zachowaniem może być projekt stosowany przez strażnika dostępu, przedstawianie użytkownikom końcowym opcji wyboru w sposób, który nie jest neutralny, lub wykorzystywanie struktury, funkcji lub sposobu obsługi interfejsu użytkownika lub jego części w celu osłabienia lub ograniczenia autonomii użytkownika, jego możliwości podejmowania decyzji lub wyboru. Ponadto należy zakazać strażnikowi dostępu dopuszczania się zachowań, które w jakikolwiek sposób osłabiają interoperacyjność wymaganą na podstawie niniejszego rozporządzenia, na przykład poprzez stosowanie nieuzasadnionych technicznych środków ochrony lub dyskryminujących warunków świadczenia usług, bezprawne zgłaszanie praw autorskich do interfejsów programowania aplikacji lub dostarczanie informacji wprowadzających w błąd. Strażnikom dostępu należy zakazać obchodzenia wskazania ich jako strażnika dostępu poprzez sztuczne dokonywanie segmentacji, podziału, dalszego podziału, fragmentacji lub rozdzielania swoich podstawowych usług platformowych w celu obejścia progów ilościowych ustanowionych w niniejszym rozporządzeniu.
- (71) Aby zapewnić skuteczność przeglądu statusu strażnika dostępu, jak również możliwość dostosowywania wykazu podstawowych usług platformowych świadczonych przez strażnika dostępu, strażnicy dostępu powinni informować Komisję o wszystkich zamierzanych przejęciach – przed ich dokonaniem – innych przedsiębiorstw świadczących podstawowe usługi platformowe lub jakiegokolwiek inne usługi świadczone w sektorze cyfrowym lub inne usługi umożliwiające zbieranie danych. Takie informacje powinny nie tylko być przydatne w procesie przeglądu dotyczącym statusu poszczególnych strażników dostępu, ale zapewnią również informacje o kluczowym znaczeniu dla monitorowania szerszych tendencji w zakresie kontestowalności w sektorze cyfrowym, w związku z czym mogą być użytecznym elementem do rozważenia w kontekście badań rynku określonych w niniejszym rozporządzeniu. Ponadto Komisja powinna przekazywać takie informacje państwom członkowskim, biorąc pod uwagę możliwość wykorzystania ich do celów krajowej kontroli łączenia przedsiębiorstw oraz jako że w pewnych okolicznościach właściwy organ krajowy może skierować te przejęcia do Komisji do celów kontroli łączenia przedsiębiorstw. Komisja powinna również publikować co roku wykaz przejęć, o których została poinformowana przez strażnika dostępu. Aby zapewnić niezbędną przejrzystość i użyteczność takich informacji do różnych celów określonych w niniejszym rozporządzeniu, strażnicy dostępu powinni dostarczyć co najmniej informacje na temat przedsiębiorstw, których dotyczy koncentracja, ich rocznego obrotu w Unii i na świecie, ich obszaru działalności, w tym działalności bezpośrednio związanej z koncentracją, wartości transakcyjnej lub jej oszacowania, skrócony opis koncentracji, w tym jej charakter i uzasadnienie, a także wykaz państw członkowskich, których dotyczy dane działanie.
- (72) Ochrona danych użytkowników końcowych oraz ich prywatności ma istotne znaczenie przy przeprowadzaniu oceny potencjalnie negatywnych skutków zaobserwowanych praktyk stosowanych przez strażników dostępu w zakresie zbierania i akumulacji dużych ilości danych pochodzących od użytkowników końcowych. Zapewnienie odpowiedniego poziomu przejrzystości stosowanych przez strażników dostępu praktyk w zakresie profilowania, obejmujących profilowanie w rozumieniu art. 4 pkt 4 rozporządzenia (UE) 2016/679, ale nieograniczonych wyłącznie do niego, ułatwia kontestowalność podstawowych usług platformowych. Przejrzystość wywiera na strażników dostępu zewnętrzną presję, aby nie czynić z głębokiego profilowania konsumentów normy w branży, biorąc pod uwagę fakt, że potencjalne nowe podmioty wchodzące na rynek lub przedsiębiorstwa typu start-up nie są w stanie uzyskać dostępu do danych w takim samym zakresie, na takim samym poziomie szczegółowości i na podobną skalę. Dzięki większej przejrzystości inne przedsiębiorstwa świadczące podstawowe usługi platformowe powinny móc łatwiej odróżnić się od pozostałych podmiotów za sprawą stosowania lepszych gwarancji ochrony prywatności.

Aby zapewnić minimalny poziom skuteczności tego obowiązku w zakresie przejrzystości, strażnicy dostępu powinni przynajmniej przedstawić poddany niezależnemu audytowi opis założeń prowadzonego profilowania, w tym informacje na temat tego, czy dane osobowe i dane uzyskane na podstawie analizy aktywności użytkownika zgodnie z rozporządzeniem (UE) 2016/679 są wykorzystywane i przetwarzane, a także informacje na temat celu, w jakim sporządza się i ostatecznie wykorzystuje profil, czasu profilowania, wpływu tego rodzaju profilowania na usługi świadczone przez strażnika dostępu oraz kroków podejmowanych w celu skutecznego zapewnienia użytkownikom końcowym wiedzy na temat odpowiedniego wykorzystania takiego profilowania, jak również kroków podejmowanych w celu uzyskania ich zgody lub w celu zapewnienia im możliwości odmowy lub cofnięcia zgody. Poddany audytowi opis Komisja powinna przekazać Europejskiej Radzie Ochrony Danych w celu wniesienia wkładu w egzekwowanie unijnych przepisów w zakresie ochrony danych. Komisja powinna być uprawniona do opracowania metodyki i procedury odnośnie do poddawanego audytowi opisu, w porozumieniu z Europejskim Inspektorem Ochrony Danych, Europejską Radą Ochrony Danych, społeczeństwem obywatelskim i ekspertami, zgodnie z rozporządzeniami Parlamentu Europejskiego i Rady (UE) nr 182/2011<sup>(16)</sup> i (UE) 2018/1725<sup>(17)</sup>.

- (73) Aby zapewnić pełne i trwale osiągnięcie celów niniejszego rozporządzenia, Komisja powinna mieć możliwość dokonywania oceny, czy przedsiębiorstwo świadczące podstawowe usługi platformowe powinno zostać wskazane jako strażnik dostępu mimo nieosiągnięcia progów ilościowych ustanowionych w niniejszym rozporządzeniu; czy systematyczne niewypełnianie obowiązków przez strażnika dostępu daje podstawy do zastosowania dodatkowych środków zaradczych; czy do wykazu podstawowych usług platformowych należy dodać więcej usług; oraz czy należy zbadać inne, podobnie nieuczciwe praktyki ograniczające kontestowalność rynków cyfrowych. Taka ocena powinna opierać się na badaniach rynku przeprowadzanych w odpowiednich ramach czasowych, z zastosowaniem przejrzystych procedur i jasno określonych terminów, aby wzmocnić wpływ *ex ante* niniejszego rozporządzenia na kontestowalność i uczciwość w sektorze cyfrowym oraz zapewnić wymagany poziom pewności prawa.
- (74) Po przeprowadzeniu badania rynku Komisja powinna mieć możliwość stwierdzenia, czy przedsiębiorstwo świadczące podstawową usługę platformową spełnia wszystkie nadrzędne kryteria jakościowe, aby uznać je za strażnika dostępu. Przedsiębiorstwo to powinno zatem – co do zasady – wypełniać wszystkie stosowne obowiązki ustanowione w niniejszym rozporządzeniu. Jednak w przypadku strażników dostępu, którzy zostali wskazani przez Komisję, ponieważ można przewidzieć, że w niedalekiej przyszłości zajmą ugruntowaną i trwałą pozycję, Komisja powinna nakładać tylko te obowiązki, które są konieczne i stosowne do zapobieżenia osiągnięciu przez strażnika dostępu ugruntowanej i trwałej pozycji w zakresie prowadzonej przez niego działalności. W przypadku takich nowo powstających strażników dostępu, Komisja powinna wziąć pod uwagę fakt, że status ten ma co do zasady tymczasowy charakter, dlatego też w odpowiednim momencie należy zdecydować, czy na dane przedsiębiorstwo świadczące podstawowe usługi platformowe należy nałożyć pełen zbiór obowiązków strażnika dostępu z uwagi na fakt, że osiągnęło ono ugruntowaną i trwałą pozycję, czy też należy znieść wszystkie nałożone wcześniej obowiązki z uwagi na fakt, że warunki wskazania nie zostały ostatecznie spełnione.
- (75) Komisja powinna zbadać i ocenić, czy zastosowanie dodatkowych behawioralnych lub – w stosownych przypadkach – strukturalnych środków zaradczych jest uzasadnione, aby uniemożliwić strażnikowi dostępu utrudnianie osiągnięcia celów niniejszego rozporządzenia przez systematyczne niewypełnianie co najmniej jednego z obowiązków ustanowionych w niniejszym rozporządzeniu. Ma to miejsce w przypadku, gdy Komisja wydała wobec danego strażnika dostępu w okresie 8 lat co najmniej trzy decyzje stwierdzające niewypełnianie obowiązków, które mogą dotyczyć różnych podstawowych usług platformowych i różnych obowiązków ustanowionych w niniejszym rozporządzeniu, oraz gdy strażnik dostępu utrzymał, rozszerzył lub umocnił swoje oddziaływanie na rynku wewnętrznym, ekonomiczną zależność użytkowników biznesowych oraz użytkowników końcowych od swoich podstawowych usług platformowych lub jeszcze bardziej ugruntował swoją pozycję. Uznaje się, że strażnik dostępu utrzymał, rozszerzył lub umocnił swoją pozycję strażnika dostępu, w przypadku gdy – pomimo podjętych przez Komisję działań w zakresie egzekwowania prawa – utrzymał, zwiększył lub ugruntował swoje znaczenie jako punkt dostępu dla użytkowników biznesowych, za pośrednictwem którego docierają oni do użytkowników końcowych.

<sup>(16)</sup> 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).

<sup>(17)</sup> 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).

W takich przypadkach Komisja powinna być uprawniona do zastosowania dowolnego środka zaradczego niezależnie od tego, czy ma on charakter behawioralny czy strukturalny, z należyтым uwzględnieniem zasady proporcjonalności. W tym kontekście Komisja powinna być uprawniona do wprowadzenia – w zakresie, w jakim taki środek zaradczy jest proporcjonalny i konieczny do utrzymania lub przywrócenia uczciwości i kontestowalności, na które wpływa systematyczne niewypełnianie obowiązków – obowiązującego przez ograniczony okres zakazu zawierania przez danego strażnika dostępu umów dotyczących koncentracji w odniesieniu do tych podstawowych usług platformowych lub innych usług świadczonych w sektorze cyfrowym lub umożliwiających zbieranie danych, na które wpływa systematyczne niewypełnianie obowiązków. Aby umożliwić faktyczne zaangażowanie osób trzecich oraz przetestowanie środków zaradczych przed ich zastosowaniem, Komisja powinna opublikować szczegółowe jawne streszczenie opisujące daną sprawę i środki, jakie zamierza podjąć. Komisja powinna mieć możliwość wznowienia postępowania, również w przypadku gdy doprecyzowane środki zaradcze okażą się nieskuteczne. Wznowienie ze względu na nieskuteczność środków zaradczych przyjętych w drodze decyzji powinno umożliwić Komisji perspektywną zmianę tych środków zaradczych. Komisja powinna również mieć możliwość określenia rozsądnego okresu, w którym można wznowić postępowanie, jeżeli środki zaradcze okażą się nieskuteczne.

- (76) Jeżeli w toku badania dotyczącego systematycznego niewypełniania obowiązków strażnik dostępu proponuje Komisji, iż podjęcie się określonych zobowiązań, Komisja powinna mieć możliwość przyjęcia decyzji, na mocy której zobowiązania te stałyby się wiążące dla danego strażnika dostępu, jeżeli uzna, że zobowiązania te zapewniają skuteczne wypełnianie obowiązków ustanowionych w niniejszym rozporządzeniu. W decyzji takiej należy również stwierdzić, że w danym przypadku nie ma już podstaw do prowadzenia przez Komisję badania dotyczącego systematycznego niewypełniania obowiązków. Oceniając, czy zobowiązania zaproponowane przez strażnika dostępu są wystarczające, by zapewnić skuteczne wypełnianie obowiązków ustanowionych w niniejszym rozporządzeniu, Komisja powinna mieć możliwość uwzględnienia testów przeprowadzonych przez strażnika dostępu w celu wykazania w praktyce skuteczności proponowanych zobowiązań. Komisja powinna sprawdzić, czy decyzja dotycząca zobowiązań jest w pełni przestrzegana i czy realizowane są jej cele, a także powinna być uprawniona do ponownego rozpatrzenia tej decyzji, jeżeli stwierdzi, że zobowiązania nie są skuteczne.
- (77) Usługi w sektorze cyfrowym i rodzaje praktyk odnoszących się do tych usług mogą szybko i istotnie się zmieniać. Aby zapewnić aktualność niniejszego rozporządzenia i zagwarantować, że będzie ono stanowiło podstawę do podejmowania skutecznych i kompleksowych działań regulacyjnych w odpowiedzi na problemy stwarzane przez strażników dostępu, należy dokonywać regularnego przeglądu wykazów podstawowych usług platformowych, jak również obowiązków określonych w niniejszym rozporządzeniu. Ma to szczególnie istotne znaczenie dla zapewnienia zidentyfikowania praktyki, która prawdopodobnie ograniczy kontestowalność podstawowych usług platformowych lub która jest nieuczciwa. Choć przeprowadzanie przeglądów w regularnych odstępach czasu jest istotne – zważywszy na dynamicznie zmieniający się charakter sektora cyfrowego – to zapewnienie pewności prawa w kwestii warunków regulacyjnych wiąże się z koniecznością przeprowadzania przeglądów w rozsądnych i odpowiednich terminach. Badania rynku powinny również dostarczyć Komisji solidnej podstawy dowodowej pozwalającej ocenić, czy należy przedstawić wniosek dotyczący zmiany niniejszego rozporządzenia w celu dokonania przeglądu, rozszerzenia lub doprecyzowania wykazów podstawowych usług platformowych. Badania te powinny również dostarczyć Komisji solidnej podstawy dowodowej pozwalającej ocenić, czy należy przedstawić wniosek dotyczący zmiany obowiązków ustanowionych w niniejszym rozporządzeniu lub przyjąć akt delegowany aktualizujący takie obowiązki.
- (78) W odniesieniu do praktyk strażników dostępu, które nie wchodzą w zakres obowiązków ustanowionych w niniejszym rozporządzeniu, Komisja powinna mieć możliwość rozpoczęcia badania rynku dotyczącego nowych usług i nowych praktyk w celu ustalenia, czy obowiązki określone w niniejszym rozporządzeniu należy uzupełnić w drodze aktu delegowanego, który wchodzi w zakres upoważnienia określony dla takich aktów delegowanych w niniejszym rozporządzeniu, lub poprzez przedstawienie wniosku w sprawie zmiany niniejszego rozporządzenia. Pozostaje to bez uszczerbku dla możliwości wszczęcia przez Komisję, w stosownych przypadkach, postępowań na podstawie art. 101 lub 102 TFUE. Takie postępowania powinny być prowadzone zgodnie z rozporządzeniem Rady (WE) nr 1/2003<sup>(18)</sup>. W pilnych przypadkach ze względu na ryzyko wystąpienia poważnej i nieodwracalnej szkody dla konkurencji Komisja powinna rozważyć przyjęcie środków tymczasowych zgodnie z art. 8 rozporządzenia (WE) nr 1/2003.

<sup>(18)</sup> Rozporządzenie Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu (Dz.U. L 1 z 4.1.2003, s. 1).

- (79) Jeżeli strażnicy dostępu dopuszczają się praktyki, która jest nieuczciwa lub ogranicza kontestowalność podstawowych usług platformowych, które zostały już wskazane na podstawie niniejszego rozporządzenia, ale praktyki takie nie zostały wyraźnie objęte obowiązkami ustanowionymi w niniejszym rozporządzeniu, Komisja powinna mieć możliwość zaktualizowania niniejszego rozporządzenia w drodze aktów delegowanych. Tego rodzaju aktualizacje w drodze aktu delegowanego powinny podlegać tej samej normie badawczej, a zatem powinno je poprzedzać badanie rynku. Komisja powinna również identyfikować takie rodzaje praktyk, stosując uprzednio zdefiniowaną normę. Ta norma prawna powinna gwarantować dostateczny poziom przewidywalności w zakresie rodzaju obowiązków, które mogą zostać w dowolnym momencie nałożone na strażników dostępu na podstawie niniejszego rozporządzenia.
- (80) Aby zapewnić skuteczne wykonywanie niniejszego rozporządzenia i przestrzeganie jego przepisów, Komisja powinna dysponować szerokimi uprawnieniami w zakresie prowadzenia badań i egzekwowania, umożliwiającymi jej badanie, egzekwowanie i monitorowanie zgodności z przepisami niniejszego rozporządzenia przy jednoczesnym zapewnieniu poszanowania prawa podstawowego do bycia wysłuchanym oraz prawa dostępu do akt sprawy w toku postępowania dotyczącego egzekwowania przepisów. Komisja powinna korzystać z tych uprawnień w zakresie prowadzenia badań również w celu przeprowadzania badań rynku, w tym na potrzeby aktualizacji i przeglądu niniejszego rozporządzenia.
- (81) Komisja powinna być uprawniona do zwracania się o udzielenie jej informacji niezbędnych do celów niniejszego rozporządzenia. Komisja powinna mieć w szczególności dostęp do wszelkich istotnych dokumentów, danych, baz danych, algorytmów i informacji niezbędnych do rozpoczęcia i prowadzenia badań oraz monitorowania wypełniania obowiązków ustanowionych w niniejszym rozporządzeniu niezależnie od tego, kto jest w posiadaniu takich informacji, oraz niezależnie od tego, w jakiej są formie lub w jakim formacie, na jakim nośniku lub w jakim miejscu są przechowywane.
- (82) Komisja powinna mieć możliwość bezpośredniego zwracania się do przedsiębiorstw lub związków przedsiębiorstw o przekazanie wszelkich istotnych dowodów, danych i informacji. Ponadto na potrzeby niniejszego rozporządzenia Komisja powinna mieć możliwość zwracania się o wszelkie istotne informacje do właściwych organów państw członkowskich lub do dowolnej osoby fizycznej lub prawnej. Wykonując decyzję Komisji, przedsiębiorstwa są zobowiązane do udzielenia odpowiedzi na pytania dotyczące okoliczności faktycznych oraz do przedstawienia dokumentów.
- (83) Komisja powinna być również uprawniona do przeprowadzania kontroli wszelkich przedsiębiorstw lub związków przedsiębiorstw oraz do odbierania wyjaśnień od wszelkich osób mogących znajdować się w posiadaniu przydatnych informacji oraz rejestrowania złożonych przez nie oświadczeń.
- (84) Środki tymczasowe mogą być ważnym narzędziem zapewniającym, aby w trakcie trwającego badania naruszenie będące jego przedmiotem nie spowodowało poważnej i nieodwracalnej szkody dla użytkowników biznesowych lub użytkowników końcowych strażników dostępu. Narzędzie to jest ważne, aby nie doprowadzić do zmian, które byłoby bardzo trudno odwrócić za pomocą decyzji Komisji przyjmowanej na zakończenie postępowania. Komisja powinna zatem mieć uprawnienia do zarządzania środkami tymczasowymi w ramach postępowania wszczętego z myślą o ewentualnym przyjęciu decyzji stwierdzającej niewypełnianie obowiązków. Uprawnienie to powinno mieć zastosowanie w przypadkach, w których Komisja stwierdziła *prima facie* naruszenie obowiązków przez strażników dostępu i gdy istnieje ryzyko zaistnienia poważnej i nienaprawialnej szkody dla użytkowników biznesowych lub użytkowników końcowych strażników dostępu. Środki tymczasowe powinny obowiązywać wyłącznie przez czas oznaczony, który upływa wraz z zakończeniem postępowania przez Komisję, albo w ustalonym okresie, który może zostać przedłużony, jeżeli to konieczne i stosowne.
- (85) Komisja powinna mieć możliwość podejmowania działań koniecznych do monitorowania skutecznego wdrażania i wypełniania obowiązków ustanowionych w niniejszym rozporządzeniu. Takie działania powinny obejmować przyznanie Komisji możliwości powoływania niezależnych ekspertów zewnętrznych oraz audytorów udzielających jej wsparcia w tym procesie – w stosownych przypadkach wspomniani eksperci i audytorzy mogą pochodzić z właściwych organów państw członkowskich, takich jak organy ochrony danych lub konsumentów. Powołując audytorów, Komisja powinna zapewnić wystarczającą rotację.

- (86) Wypełnianie obowiązków nałożonych niniejszym rozporządzeniem powinno być egzekwowane za pośrednictwem grzywien i okresowych kar pieniężnych. W tym celu należy określić także odpowiednie poziomy grzywien i okresowych kar pieniężnych za niewypełnianie obowiązków i naruszanie przepisów proceduralnych, z zastrzeżeniem odpowiednich terminów przedawnienia, zgodnie z zasadami proporcjonalności i *ne bis in idem*. Aby zapewnić poszanowanie tych zasad, Komisja i odpowiednie organy krajowe powinny koordynować swoje wysiłki w zakresie egzekwowania. W szczególności Komisja powinna uwzględniać wszelkie grzywny i sankcje nałożone na tę samą osobę prawną w odniesieniu do tych samych faktów w drodze ostatecznej decyzji w postępowaniu dotyczącym naruszenia innych przepisów unijnych lub krajowych, tak by zapewnić, aby łącznie nałożone grzywny i sankcje odpowiadały wadze popełnionych naruszeń.
- (87) W celu zapewnienia skutecznego ściągania grzywien nałożonych na związki przedsiębiorstw za naruszenia, jakich się dopuściły, konieczne jest ustalenie warunków, na jakich Komisja może domagać się zapłaty grzywien od członków tego związku przedsiębiorstw w przypadku jego niewypłacalności.
- (88) W ramach postępowań prowadzonych zgodnie z niniejszym rozporządzeniem zainteresowanemu przedsiębiorstwu powinno przysługiwać prawo do bycia wysłuchanym przez Komisję, a podejmowane decyzje powinny być podawane do szerokiej wiadomości. Zapewniając poszanowanie prawa do dobrej administracji, prawa dostępu do akt i prawa do bycia wysłuchanym, istotne znaczenie ma ochrona informacji poufnych. Ponadto, zachowując poufność informacji, Komisja powinna zapewnić, aby wszelkie informacje, na których opiera się jej decyzja, zostały ujawnione w zakresie, który umożliwi adresatowi decyzji zrozumienie stanu faktycznego i wnioskowania, które doprowadziły do jej podjęcia. Konieczne jest również zapewnienie, aby Komisja korzystała wyłącznie z informacji zgromadzonych na podstawie niniejszego rozporządzenia do celów niniejszego rozporządzenia, z wyjątkiem przypadków, w których określono inaczej. Wreszcie powinno być możliwe, na określonych warunkach, uznanie niektórych dokumentów dotyczących działalności przedsiębiorstwa, na przykład informacji wymienianych między prawnikami a ich klientami, za poufne, jeżeli spełniono stosowne warunki.
- (89) Przygotowując do publikacji jawne streszczenia skutecznie umożliwiające zainteresowanym osobom trzecim zgłoszenie uwag, Komisja powinna należycie uwzględnić uzasadniony interes przedsiębiorstw w zakresie ochrony ich tajemnic handlowych i innych informacji poufnych.
- (90) Spójne, skuteczne i uzupełniające się egzekwowanie dostępnych instrumentów prawnych stosowanych wobec strażników dostępu wymaga współpracy i koordynacji między Komisją a organami krajowymi w ramach ich kompetencji. Komisja i organy krajowe powinny współpracować i koordynować swoje działania niezbędne do egzekwowania dostępnych instrumentów prawnych stosowanych wobec strażników dostępu w rozumieniu niniejszego rozporządzenia oraz przestrzegać zasady lojalnej współpracy ustanowionej w art. 4 Traktatu o Unii Europejskiej (TUE). Wsparcie udzielane Komisji przez organy krajowe powinno móc obejmować dostarczanie jej wszelkich niezbędnych informacji będących w ich posiadaniu lub pomoc Komisji, na jej wniosek, w wykonywaniu jej uprawnień, tak aby mogła ona lepiej wykonywać zadania powierzone jej na podstawie niniejszego rozporządzenia.
- (91) Komisja jest jedynym organem uprawnionym do egzekwowania niniejszego rozporządzenia. W celu wsparcia Komisji państwa członkowskie powinny mieć możliwość upoważnienia swoich właściwych organów krajowych egzekwujących reguły konkurencji do prowadzenia dochodzeń dotyczących możliwego niewypełnienia przez strażników dostępu niektórych obowiązków wynikających z niniejszego rozporządzenia. Może to mieć w szczególności znaczenie w przypadkach, w których nie można z góry ustalić, czy zachowanie strażnika dostępu może stanowić naruszenie niniejszego rozporządzenia lub reguł konkurencji, do których egzekwowania uprawniony jest właściwy organ krajowy. Właściwy organ krajowy egzekwujący reguły konkurencji powinien zgłaszać Komisji swoje ustalenia dotyczące możliwego niewypełnienia przez strażników dostępu niektórych obowiązków wynikających z niniejszego rozporządzenia, tak by umożliwić Komisji, jako jednemu organowi egzekwującemu przepisy ustanowione w niniejszym rozporządzeniu, wszczęcie postępowania w celu zbadania wszelkich przypadków niewypełniania obowiązków.

Komisja powinna mieć pełną swobodę decydowania o wszczęciu takiego postępowania. Aby uniknąć nakładania się postępowań prowadzonych na podstawie niniejszego rozporządzenia, dany właściwy organ krajowy powinien poinformować Komisję przed podjęciem pierwszej czynności dochodzeniowej dotyczącej możliwego niewypełnienia przez strażników dostępu niektórych obowiązków wynikających z niniejszego rozporządzenia. Właściwe organy krajowe powinny również prowadzić ścisłą współpracę i koordynację z Komisją podczas egzekwowania krajowych reguł konkurencji względem strażników dostępu, w tym w odniesieniu do ustalania grzywnien. W tym celu powinny one informować Komisję o wszczęciu postępowań przeciwko strażnikom dostępu w oparciu o krajowe reguły konkurencji, a także przed nałożeniem obowiązków na strażników dostępu w takich postępowaniach. Aby uniknąć powielania działań, informacja o projekcie decyzji na podstawie art. 11 rozporządzenia (WE) nr 1/2003 powinna, w stosownych przypadkach, móc służyć jako powiadomienie na mocy niniejszego rozporządzenia.

- (92) W celu zagwarantowania zharmonizowanego stosowania i egzekwowania niniejszego rozporządzenia ważne jest zapewnienie, aby organy krajowe, w tym sądy krajowe, posiadały wszystkie informacje niezbędne do zapewnienia, by ich decyzje nie były sprzeczne z decyzją przyjętą przez Komisję na podstawie niniejszego rozporządzenia. Sądy krajowe powinny mieć możliwość zwrócenia się do Komisji o przesłanie im informacji lub opinii w kwestiach dotyczących stosowania niniejszego rozporządzenia. Jednocześnie Komisja powinna mieć możliwość przedstawienia sądom krajowym ustnych lub pisemnych uwag. Pozostaje to bez uszczerbku dla możliwości wystąpienia przez sądy krajowe z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym na podstawie art. 267 TFUE.
- (93) W celu zapewnienia spójnego, skutecznego i komplementarnego wykonywania niniejszego rozporządzenia oraz innych przepisów sektorowych mających zastosowanie do strażników dostępu Komisja powinna korzystać z wiedzy fachowej specjalnej grupy wysokiego szczebla. Ta grupa wysokiego szczebla powinna mieć również możliwość wspomagania Komisji poprzez doradztwo, wiedzę fachową i zalecenia, w zależności od przypadku, w ogólnych kwestiach dotyczących wykonywania lub egzekwowania niniejszego rozporządzenia. W skład grupy wysokiego szczebla powinny wchodzić odpowiednie europejskie organy i sieci, a skład tej grupy powinien zapewniać wysoki poziom wiedzy fachowej i równowagę geograficzną. Członkowie grupy wysokiego szczebla powinni regularnie składać reprezentowanym przez siebie organom i sieciom sprawozdania dotyczące zadań wykonywanych w ramach grupy i konsultować się w tym względzie z tymi organami i sieciami.
- (94) Ponieważ decyzje przyjmowane przez Komisję na podstawie niniejszego rozporządzenia podlegają kontroli Trybunału Sprawiedliwości zgodnie z TFUE, Trybunał Sprawiedliwości powinien mieć w myśl art. 261 TFUE nieograniczone prawo orzekania w odniesieniu do grzywnien i okresowych kar pieniężnych.
- (95) Komisja powinna mieć możliwość opracowania wytycznych w celu zapewnienia dalszych wskazówek dotyczących różnych aspektów niniejszego rozporządzenia lub w celu udzielenia przedsiębiorstwom świadczącym podstawowe usługi platformowe pomocy w wypełnianiu obowiązków wynikających z niniejszego rozporządzenia. Powinna w szczególności istnieć możliwość oparcia takich wskazówek na doświadczeniu uzyskanym przez Komisję w ramach monitorowania przestrzegania niniejszego rozporządzenia. Wydawanie jakichkolwiek wytycznych na podstawie niniejszego rozporządzenia jest kompetencją Komisji wykonywaną według jej wyłącznego uznania i nie powinno być uznawane za konstytutywny element zapewniania wypełniania przez przedsiębiorstwa lub związki przedsiębiorstw obowiązków wynikających z niniejszego rozporządzenia.
- (96) Wypełnianie niektórych obowiązków strażników dostępu, takich jak te związane z dostępem do danych, możliwością przenoszenia danych lub interoperacyjnością, można ułatwić poprzez stosowanie norm technicznych. W związku z tym w stosownych i koniecznych przypadkach Komisja powinna mieć możliwość zwrócenia się do europejskich organów normalizacyjnych o ich opracowanie.
- (97) W celu zapewnienia kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii, na których działają strażnicy dostępu, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w odniesieniu do zmiany metodyki ustalania, czy osiągnięte zostały progi ilościowe dotyczące aktywnych użytkowników końcowych i aktywnych użytkowników biznesowych, wykorzystywane do wskazania strażników dostępu, która to metodyka jest zawarta w załączniku do niniejszego rozporządzenia, w odniesieniu do doprecyzowania dodatkowych elementów tej metodyki nieujętych w tym załączniku służących ustaleniu, czy osiągnięte zostały progi ilościowe dotyczące wskazywania strażników dostępu, oraz w odniesieniu do uzupełnienia istniejących obowiązków ustanowionych w niniejszym rozporządzeniu, w przypadkach gdy na podstawie badania rynku Komisja stwierdziła potrzebę aktualizacji obowiązków dotyczących praktyk, które ograniczają kontestowalność podstawowych usług platformowych lub są nieuczciwe, a rozważana aktualizacja wchodzi w zakres upoważnienia określony dla takich aktów delegowanych w niniejszym rozporządzeniu.



- (98) Szczególnie ważne jest, aby Komisja przyjmując akty delegowane na podstawie niniejszego rozporządzenia prowadziła w czasie prac przygotowawczych 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<sup>(19)</sup>. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te powinny otrzymywać wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji powinni systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.
- (99) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze do określania środków, które mają być wdrożone przez strażników dostępu w celu skutecznego wypełniania obowiązków wynikających z niniejszego rozporządzenia; do zawieszenia w całości lub w części określonego obowiązku nałożonego na strażnika dostępu; do zwolnienia strażnika dostępu w całości lub w części z określonego obowiązku; do określania środków, które mają być wdrożone przez strażnika dostępu, w przypadku gdy obchodzi on obowiązki wynikające z niniejszego rozporządzenia; do zakończenia badania rynku służącego wskazaniu strażników dostępu; do nakładania środków zaradczych w przypadku systematycznego niewypełniania obowiązków; do zarządzania środkami tymczasowymi wobec strażnika dostępu; do uczynienia zobowiązań podjętych przez strażnika dostępu wiążącymi; do przedstawienia ustaleń dotyczących niewypełniania obowiązków; do ustalenia ostatecznej wysokości okresowej kary pieniężnej; do określania formy, treści i innych szczegółów powiadomień, przekazywanych informacji, uzasadnionych wniosków i obowiązkowych sprawozdań, przedkładanych przez strażników dostępu; do ustanawiania ustaleń operacyjnych i technicznych służących wdrożeniu interoperacyjności oraz metodyki i procedury odnośnie do poddanego audytowi opisu technik wykorzystywanych do profilowania konsumentów; do określania praktycznych ustaleń w odniesieniu do postępowań, przedłużania terminów, wykonywania praw w toku postępowania, warunków ujawnienia, a także współpracy i koordynacji między Komisją a organami krajowymi. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011.
- (100) W odniesieniu do przyjęcia aktu wykonawczego w sprawie praktycznych ustaleń dotyczących współpracy i koordynacji między Komisją a państwami członkowskimi należy stosować procedurę sprawdzającą. W odniesieniu do pozostałych aktów wykonawczych przewidzianych w niniejszym rozporządzeniu należy stosować procedurę doradczą. Jest to uzasadnione faktem, że pozostałe akty wykonawcze są związane z praktycznymi aspektami procedur ustanowionych w niniejszym rozporządzeniu, takimi jak forma, treść i inne szczegóły poszczególnych etapów proceduralnych, praktycznymi ustaleniami dotyczącymi różnych etapów procedury, takimi jak na przykład przedłużenie terminów proceduralnych lub prawo do bycia wysłuchanym, a także z indywidualnymi decyzjami wykonawczymi skierowanymi do strażnika dostępu.
- (101) Zgodnie z rozporządzeniem (UE) nr 182/2011 każde państwo członkowskie powinno być reprezentowane w Komitecie Doradczym i powinno decydować o składzie swojej delegacji. W skład takiej delegacji mogą wchodzić między innymi eksperci z właściwych organów w państwach członkowskich, posiadający odpowiednią wiedzę fachową dotyczącą określonej kwestii przedstawionej komitetowi doradczemu.
- (102) Sygnaliści mogą zwracać uwagę właściwych organów na nowe informacje, co może pomóc tym organom w wykrywaniu przypadków naruszenia niniejszego rozporządzenia oraz umożliwić im nakładanie sankcji. Należy zapewnić istnienie odpowiednich rozwiązań umożliwiających sygnalistom ostrzeganie właściwych organów o faktycznych lub potencjalnych naruszeniach niniejszego rozporządzenia oraz chroniących te osoby przed środkami odwetowymi. W tym celu należy określić w niniejszym rozporządzeniu, że do zgłaszania naruszeń niniejszego rozporządzenia i do ochrony osób zgłaszających takie naruszenia zastosowanie ma dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937<sup>(20)</sup>.
- (103) W celu zwiększenia pewności prawa stosowanie na podstawie niniejszego rozporządzenia dyrektywy (UE) 2019/1937 do zgłaszania naruszeń niniejszego rozporządzenia i do ochrony osób zgłaszających takie naruszenia powinno zostać uwzględnione w tej dyrektywie. Należy zatem odpowiednio zmienić załącznik do dyrektywy (UE) 2019/1937. Do państw członkowskich należy zapewnić, by zmiana ta została uwzględniona w ich środkach transpozycji przyjętych zgodnie z dyrektywą (UE) 2019/1937, niemniej przyjęcie krajowych środków transpozycji nie jest warunkiem stosowania tej dyrektywy do zgłaszania naruszeń niniejszego rozporządzenia i do ochrony osób zgłaszających takie naruszenia od dnia rozpoczęcia stosowania niniejszego rozporządzenia.

<sup>(19)</sup> Dz.U. L 123 z 12.5.2016, s. 1.

<sup>(20)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.U. L 305 z 26.11.2019, s. 17).

- (104) Konsumentom powinni być uprawnieni do wykonywania swoich praw, pozostających w związku z obowiązkami nałożonymi na strażników dostępu na mocy niniejszego rozporządzenia, w drodze powództw przedstawicielskich zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2020/1828 <sup>(21)</sup>. W tym celu w niniejszym rozporządzeniu należy określić, że do powództw przedstawicielskich wytaczanych przeciwko strażnikom dostępu za naruszenia przepisów niniejszego rozporządzenia szkodzące lub mogące szkodzić zbiorowym interesom konsumentów zastosowanie ma dyrektywa (UE) 2020/1828. Należy zatem odpowiednio zmienić załącznik do tej dyrektywy. Do państw członkowskich należy zapewnić, by zmiana ta została uwzględniona w ich środkach transpozycji przyjętych zgodnie z dyrektywą (UE) 2020/1828, niemniej przyjęcie krajowych środków transpozycji nie jest warunkiem stosowania tej dyrektywy do tych powództw przedstawicielskich. Stosowanie dyrektywy (UE) 2020/1828 do powództw przedstawicielskich wytaczanych przeciwko strażnikom dostępu za naruszenia przepisów niniejszego rozporządzenia szkodzące lub mogące szkodzić zbiorowym interesom konsumentów zaczyna się od daty rozpoczęcia stosowania ustawowych, wykonawczych i administracyjnych przepisów państw członkowskich, które są niezbędne do transpozycji tej dyrektywy, lub od daty rozpoczęcia stosowania niniejszego rozporządzenia, w zależności od tego, co nastąpi później.
- (105) Komisja powinna dokonywać okresowo oceny niniejszego rozporządzenia oraz ściśle monitorować jego skutki dla contestowalności i uczciwości stosunków handlowych w ramach gospodarki platform internetowych, w szczególności w celu ustalenia, czy istnieje potrzeba wprowadzenia zmian w świetle istotnego rozwoju sytuacji w dziedzinie technologii lub handlu. Aby zapewnić contestowalne i uczciwe rynki cyfrowe w całej Unii, ocena ta powinna obejmować dokonywanie regularnego przeglądu wykazu podstawowych usług platformowych oraz obowiązków spoczywających na strażnikach dostępu, a także działań służących egzekwowaniu wypełniania tych obowiązków. W tym kontekście Komisja powinna również oceniać zakres obowiązku dotyczącego interoperacyjności usług łączności elektronicznej niewykorzystujących numerów. W celu uzyskania szerokiego obrazu rozwoju sytuacji w sektorze cyfrowym, ocena powinna uwzględniać doświadczenia państw członkowskich i odpowiednich zainteresowanych stron. W tym względzie Komisja powinna mieć również możliwość wzięcia pod uwagę opinii i sprawozdań przekazanych jej przez Obserwatorium Gospodarki Platform Internetowych, które ustanowiono pierwotnie na mocy decyzji Komisji C(2018) 2393 z dnia 26 kwietnia 2018 r. Po dokonaniu oceny Komisja powinna podjąć stosowne działania. Przy przeprowadzaniu ocen i dokonywaniu przeglądów praktyk i obowiązków ustanowionych w niniejszym rozporządzeniu Komisja powinna dążyć do utrzymania wysokiego poziomu ochrony i poszanowania wspólnych praw i wartości, w szczególności równości i niedyskryminacji.
- (106) Bez uszczerbku dla procedury budżetowej i za pośrednictwem istniejących instrumentów finansowych należy przydzielić Komisji odpowiednie zasoby ludzkie, finansowe i techniczne, by zapewnić jej możliwość skutecznego wykonywania zadań i uprawnień w zakresie egzekwowania niniejszego rozporządzenia.
- (107) Ponieważ cel niniejszego rozporządzenia, a mianowicie zapewnienie contestowalnego i uczciwego sektora cyfrowego w ogóle, a w szczególności contestowalnych i uczciwych podstawowych usług platformowych z myślą o promowaniu innowacyjności, wysokiej jakości produktów i usług cyfrowych, uczciwych i konkurencyjnych cen, a także wysokiej jakości i swobody wyboru dla użytkowników końcowych w sektorze cyfrowym, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast z uwagi na model biznesowy strażników dostępu i charakter prowadzonej przez nich działalności oraz skalę i skutki tej działalności, możliwe jest lepsze osiągnięcie tego celu na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.
- (108) Zgodnie z art. 42 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 10 lutego 2021 r. <sup>(22)</sup>
- (109) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej, w szczególności w jej art. 16, 47 i 50. Przy wykładni i stosowaniu niniejszego rozporządzenia te prawa i zasady powinny być odpowiednio przestrzegane,

<sup>(21)</sup> 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).

<sup>(22)</sup> Dz.U. C 147 z 26.4.2021, s. 4.

PRZYMUJĄ NINIEJSZE ROZPORZĄDZENIE:

## ROZDZIAŁ I

### PRZEDMIOT, ZAKRES STOSOWANIA I DEFINICJE

#### Artykuł 1

##### Przedmiot i zakres stosowania

1. Celem niniejszego rozporządzenia jest przyczynienie się do prawidłowego funkcjonowania rynku wewnętrznego poprzez ustanowienie zharmonizowanych przepisów służących zapewnieniu wszystkim przedsiębiorstwom kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii, na których działają strażnicy dostępu, z korzyścią dla użytkowników biznesowych i użytkowników końcowych.
2. Niniejsze rozporządzenie stosuje się do podstawowych usług platformowych świadczonych lub oferowanych przez strażników dostępu użytkownikom biznesowym mającym siedzibę w Unii lub użytkownikom końcowym mającym siedzibę lub miejsce pobytu w Unii, niezależnie od siedziby lub miejsca pobytu strażników dostępu i niezależnie od innych przepisów prawa mających zastosowanie do świadczenia usług.
3. Niniejszego rozporządzenia nie stosuje się do rynków związanych z:
  - a) sieciami łączności elektronicznej zdefiniowanymi w art. 2 pkt 1 dyrektywy (UE) 2018/1972;
  - b) usługami łączności elektronicznej zdefiniowanymi w art. 2 pkt 4 dyrektywy (UE) 2018/1972, z wyjątkiem usług łączności interpersonalnej niewykorzystujących numerów.
4. W odniesieniu do usług łączności interpersonalnej, zdefiniowanych w art. 2 pkt 5 dyrektywy (UE) 2018/1972, niniejsze rozporządzenie pozostaje bez uszczerbku dla uprawnień i zakresu odpowiedzialności powierzonych krajowym organom regulacyjnym i innym właściwym organom na mocy art. 61 tej dyrektywy.
5. W celu zapobieżenia fragmentacji rynku wewnętrznego państwa członkowskie nie mogą nakładać na strażników dostępu – w drodze środków ustawowych, wykonawczych lub administracyjnych – dodatkowych obowiązków do celów zapewnienia kontestowalnych i uczciwych rynków. Żaden z przepisów niniejszego rozporządzenia nie uniemożliwia państwu członkowskiemu nakładania na przedsiębiorstwa – w tym przedsiębiorstwa świadczące podstawowe usługi platformowe – obowiązków w odniesieniu do spraw wykraczających poza zakres stosowania niniejszego rozporządzenia, pod warunkiem że obowiązki te są zgodne z prawem Unii i nie wynikają z faktu posiadania przez odpowiednie przedsiębiorstwa statusu strażnika dostępu w rozumieniu niniejszego rozporządzenia.
6. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania art. 101 i 102 TFUE. Pozostaje ono również bez uszczerbku dla stosowania:
  - a) krajowych reguł konkurencji zakazujących antykonkurencyjnych porozumień, decyzji związków przedsiębiorstw, praktyk uzgodnionych i nadużyć pozycji dominującej;
  - b) krajowych reguł konkurencji zakazujących innych form praktyk jednostronnych w zakresie, w jakim mają one również zastosowanie do przedsiębiorstw innych niż strażnicy dostępu lub w jakim wiążą się z nałożeniem dodatkowych obowiązków na strażników dostępu; oraz
  - c) rozporządzenia Rady (WE) nr 139/2004 <sup>(23)</sup> i przepisów krajowych dotyczących kontroli łączenia przedsiębiorstw.

<sup>(23)</sup> Rozporządzenie Rady (WE) nr 139/2004 z dnia 20 stycznia 2004 r. w sprawie kontroli koncentracji przedsiębiorstw (rozporządzenie WE w sprawie kontroli łączenia przedsiębiorstw) (Dz.U. L 24 z 29.1.2004, s. 1).

7. Organy krajowe nie mogą podejmować decyzji sprzecznych z decyzją przyjętą przez Komisję na podstawie niniejszego rozporządzenia. Komisja i państwa członkowskie ściśle współpracują i koordynują swoje działania w zakresie egzekwowania w oparciu o zasady ustanowione w art. 37 i 38.

## Artykuł 2

### Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

- 1) „strażnik dostępu” oznacza przedsiębiorstwo świadczące podstawowe usługi platformowe, które wskazano na podstawie art. 3;
- 2) „podstawowa usługa platformowa” oznacza którąkolwiek z następujących usług:
  - a) usługi pośrednictwa internetowego;
  - b) wyszukiwarki internetowe;
  - c) internetowe serwisy społecznościowe;
  - d) usługi platformy udostępniania wideo;
  - e) usługi łączności interpersonalnej niewykorzystujące numerów;
  - f) systemy operacyjne;
  - g) przeglądarki internetowe;
  - h) wirtualni asystenci;
  - i) usługi przetwarzania w chmurze;
  - j) internetowe usługi reklamowe, w tym sieci reklamowe, giełdy reklamowe i inne usługi pośrednictwa w zakresie reklam, świadczone przez przedsiębiorstwo, które świadczy dowolne podstawowe usługi platformowe wymienione w lit. a)–i);
- 3) „usługa społeczeństwa informacyjnego” oznacza usługę zdefiniowaną w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535;
- 4) „sektor cyfrowy” oznacza sektor produktów dostarczanych i usług świadczonych przy użyciu lub za pośrednictwem usług społeczeństwa informacyjnego;
- 5) „usługi pośrednictwa internetowego” oznaczają usługi pośrednictwa internetowego zdefiniowane w art. 2 pkt 2 rozporządzenia (UE) 2019/1150;
- 6) „wyszukiwarka internetowa” oznacza wyszukiwarkę internetową zdefiniowaną w art. 2 pkt 5 rozporządzenia (UE) 2019/1150;
- 7) „internetowy serwis społecznościowy” oznacza platformę umożliwiającą użytkownikom końcowym łączenie się i komunikowanie ze sobą, udostępnianie treści oraz zapoznawanie się z innymi użytkownikami i treściami z wykorzystaniem różnych urządzeń, w szczególności za pośrednictwem czatów, postów, filmów wideo i rekomendacji;
- 8) „usługa platformy udostępniania wideo” oznacza usługę platformy udostępniania wideo zdefiniowaną w art. 1 ust. 1 lit. aa) dyrektywy 2010/13/UE;
- 9) „usługa łączności interpersonalnej niewykorzystująca numerów” oznacza usługę łączności interpersonalnej niewykorzystującą numerów zdefiniowaną w art. 2 pkt 7 dyrektywy (UE) 2018/1972;
- 10) „system operacyjny” oznacza oprogramowanie systemowe kontrolujące podstawowe funkcje sprzętu lub oprogramowania i zapewniające środowisko, w którym mogą działać aplikacje;
- 11) „przeglądarka internetowa” oznacza aplikację, która umożliwia użytkownikom końcowym uzyskanie dostępu do treści internetowych znajdujących się na serwerach, które są podłączone do sieci, takich jak internet, oraz interakcję z takimi treściami, w tym autonomiczne przeglądarki internetowe, a także przeglądarki internetowe zintegrowane z oprogramowaniem, wbudowane w oprogramowanie lub podobne;

- 12) „wirtualny asystent” oznacza oprogramowanie, które może przetwarzać polecenia, zadania lub pytania, w tym mające postać dźwiękową, wizualną, pisemną lub wyrażone w formie gestów lub ruchów, oraz które – w oparciu o te polecenia, zadania lub pytania – udziela dostępu do innych usług lub kontroluje podłączone urządzenia fizyczne;
- 13) „usługa przetwarzania w chmurze” oznacza usługę przetwarzania w chmurze zdefiniowaną w art. 4 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 <sup>(24)</sup>;
- 14) „sklepy z aplikacjami” oznaczają rodzaj usług pośrednictwa internetowego, w ramach których produktami lub usługami będącymi przedmiotem pośrednictwa są aplikacje;
- 15) „aplikacja” oznacza produkt cyfrowy lub usługę cyfrową, które działają w ramach systemu operacyjnego;
- 16) „usługa płatnicza” oznacza usługę płatniczą zdefiniowaną w art. 4 pkt 3 dyrektywy (UE) 2015/2366;
- 17) „usługa techniczna wspierająca usługi płatnicze” oznacza usługę w rozumieniu art. 3 lit. j) dyrektywy (UE) 2015/2366;
- 18) „system płatności za zakupy wewnątrz aplikacji” oznacza aplikację, usługę lub interfejs użytkownika, które ułatwiają dokonywanie zakupu treści cyfrowych lub usług cyfrowych wewnątrz aplikacji, w tym zakupu treści, subskrypcji, funkcji lub funkcjonalności, oraz dokonywanie płatności za takie zakupy;
- 19) „usługa identyfikacyjna” oznacza rodzaj usługi, świadczonej wraz z podstawowymi usługami platformowymi lub wspierającej takie usługi, która umożliwia dowolny rodzaj weryfikacji tożsamości użytkowników końcowych lub użytkowników biznesowych, niezależnie od wykorzystywanej technologii;
- 20) „użytkownik końcowy” oznacza osobę fizyczną lub prawną, która korzysta z podstawowych usług platformowych w charakterze innym niż użytkownik biznesowy;
- 21) „użytkownik biznesowy” oznacza osobę fizyczną lub prawną działającą w celach handlowych lub zawodowych, która korzysta z podstawowych usług platformowych do celów związanych z dostarczaniem towarów użytkownikom końcowym lub świadczeniem usług na rzecz użytkowników końcowych lub w toku dostarczania towarów takim użytkownikom lub świadczenia usług na ich rzecz;
- 22) „plasowanie” oznacza przyznawanie określonej widoczności towarom lub usługom oferowanym w ramach usług pośrednictwa internetowego, internetowych serwisów społecznościowych, usług platformy udostępniania wideo lub wirtualnych asystentów, lub nadawanie wagi wynikom wyszukiwania przez wyszukiwarki internetowe, w formie, w jakiej plasowanie to zostało przedstawione, zorganizowane lub przekazane przez przedsiębiorstwa świadczące usługi pośrednictwa internetowego, usługi internetowych serwisów społecznościowych, usługi platformy udostępniania wideo, usługi wirtualnych asystentów lub wyszukiwarek internetowych, niezależnie od środków technologicznych wykorzystanych do takiego przedstawienia, zorganizowania lub przekazania oraz niezależnie od tego, czy przedstawiany lub przekazywany jest tylko jeden wynik;
- 23) „wyniki wyszukiwania” oznaczają wszelkie informacje w dowolnym formacie, w tym formie tekstu, grafiki, w formacie głosowym lub innym, udzielone w odpowiedzi na zapytanie i związane z tym zapytaniem, niezależnie od tego, czy udzielone informacje są wynikiem płatnym lub bezpłatnym, bezpośrednią odpowiedzią lub produktem, usługą lub informacjami oferowanymi w związku z wynikami organicznymi lub wyświetlanymi wraz z nimi lub częściowo lub całkowicie w nich zawartymi;
- 24) „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;
- 25) „dane osobowe” oznaczają dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;
- 26) „dane nieosobowe” oznaczają dane inne niż dane osobowe;
- 27) „przedsiębiorstwo” oznacza podmiot prowadzący działalność gospodarczą, niezależnie od jego formy prawnej oraz sposobu jego finansowania, w tym wszystkie powiązane lub połączone przedsiębiorstwa, które tworzą grupę z uwagi na fakt, że jedno przedsiębiorstwo sprawuje bezpośrednią lub pośrednią kontrolę nad innym przedsiębiorstwem;

<sup>(24)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

- 28) „kontrola” oznacza możliwość wywierania decydującego wpływu na przedsiębiorstwo w rozumieniu art. 3 ust. 2 rozporządzenia (WE) nr 139/2004;
- 29) „interoperacyjność” oznacza zdolność w zakresie wymiany informacji i wzajemnego korzystania z informacji, których wymiany dokonano za pośrednictwem interfejsów lub innych rozwiązań, pozwalającą zapewnić, by wszystkie elementy sprzętu lub oprogramowania współdziałały z innym sprzętem i oprogramowaniem oraz z użytkownikami we wszelkich formach działania, do jakich są przeznaczone;
- 30) „obróć” oznacza uzyskaną przez przedsiębiorstwo kwotę w rozumieniu art. 5 ust. 1 rozporządzenia (WE) nr 139/2004;
- 31) „profilowanie” oznacza profilowanie zdefiniowane w art. 4 pkt 4 rozporządzenia (UE) 2016/679;
- 32) „zgoda” oznacza zgodę zdefiniowaną w art. 4 pkt 11 rozporządzenia (UE) 2016/679;
- 33) „sąd krajowy” oznacza sąd państwa członkowskiego w rozumieniu art. 267 TFUE.

## ROZDZIAŁ II

### STRAŻNICY DOSTĘPU

#### Artykuł 3

#### Wskazanie strażników dostępu

1. Przedsiębiorstwo wskazuje się jako strażnika dostępu, jeżeli:
  - a) wywiera znaczący wpływ na rynek wewnętrzny;
  - b) świadczy podstawową usługę platformową będącą ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych; oraz
  - c) zajmuje ugruntowaną i trwałą pozycję w zakresie prowadzonej przez siebie działalności lub można przewidzieć, że zajmie taką pozycję w niedalekiej przyszłości.
2. Domniemuje się, że przedsiębiorstwo spełnia odpowiednie wymogi określone w ust. 1:
  - a) w odniesieniu do ust. 1 lit. a) – jeżeli uzyskało roczny obrót w Unii wynoszący co najmniej 7,5 mld EUR w każdym z ostatnich trzech lat obrotowych lub jeżeli jego średnia kapitalizacja rynkowa lub równoważna rzeczywista wartość rynkowa wynosiła co najmniej 75 mld EUR w ostatnim roku obrotowym oraz świadczy tę samą podstawową usługę platformową w co najmniej trzech państwach członkowskich;
  - b) w odniesieniu do ust. 1 lit. b) – jeżeli świadczy podstawową usługę platformową, z której w ostatnim roku obrotowym korzystało co najmniej 45 mln aktywnych miesięcznie użytkowników końcowych mających siedzibę lub miejsce pobytu w Unii oraz co najmniej 10 000 aktywnych rocznie użytkowników biznesowych z siedzibą w Unii, przy czym użytkowników tych identyfikuje się i oblicza się ich liczbę zgodnie z metodyką i wskaźnikami określonymi w załączniku;
  - c) w odniesieniu do ust. 1 lit. c) – jeżeli progi ustanowione w lit. b) niniejszego ustępu zostały osiągnięte w każdym z ostatnich trzech lat obrotowych.
3. W przypadku gdy przedsiębiorstwo świadczące podstawowe usługi platformowe osiągnie wszystkie progi ustanowione w ust. 2, powiadamia o tym Komisję bezzwłocznie, a w każdym razie w terminie dwóch miesięcy od dnia osiągnięcia tych progów, i przedstawia jej stosowne informacje określone w ust. 2. Takie powiadomienie zawiera stosowne informacje określone w ust. 2 odnoszące się do każdej z podstawowych usług platformowych świadczonych przez przedsiębiorstwo, która osiąga progi ustanowione w ust. 2 lit. b). Za każdym razem, gdy kolejna podstawowa usługa platformowa świadczona przez przedsiębiorstwo uprzednio wskazane jako strażnik dostępu osiąga progi ustanowione w ust. 2 lit. b) i c), przedsiębiorstwo takie powiadamia o tym Komisję w terminie dwóch miesięcy od dnia osiągnięcia tych progów.

W przypadku gdy przedsiębiorstwo świadczące podstawową usługę platformową nie powiadomi Komisji na podstawie akapitu pierwszego niniejszego ustępu i nie udzieli Komisji – w terminie określonym przez nią we wniosku o udzielenie informacji na podstawie art. 21 – wszystkich stosownych informacji wymaganych przez nią do wskazania danego przedsiębiorstwa jako strażnika dostępu na podstawie ust. 4 niniejszego artykułu, Komisja pozostaje uprawniona do wskazania tego przedsiębiorstwa jako strażnika dostępu w oparciu o informacje, którymi dysponuje.

W przypadku gdy przedsiębiorstwo świadczące podstawowe usługi platformowe zastosuje się do wniosku o udzielenie informacji na podstawie akapitu drugiego niniejszego ustępu lub gdy udzieli informacji po upływie terminu, o którym mowa w tym akapicie, Komisja stosuje procedurę określoną w ust. 4.

4. Komisja – bez zbędnej zwłoki i najpóźniej w terminie 45 dni roboczych od dnia otrzymania kompletnych informacji, o których mowa w ust. 3 – wskazuje jako strażnika dostępu przedsiębiorstwo świadczące podstawowe usługi platformowe, które osiągnęło wszystkie progi ustanowione w ust. 2.

5. Przedsiębiorstwo świadczące podstawowe usługi platformowe może przedstawić, wraz z powiadomieniem, dostatecznie uzasadnione argumenty w celu wykazania, że na zasadzie wyjątku, choć osiągnęło wszystkie progi określone w ust. 2, to ze względu na okoliczności, w których świadczy odpowiednią podstawową usługę platformową, nie spełnia wymogów wymienionych w ust. 1.

W przypadku gdy Komisja uzna, że argumenty przedstawione na podstawie akapitu pierwszego przez przedsiębiorstwo świadczące podstawowe usługi platformowe nie są dostatecznie uzasadnione, ponieważ nie podważają w wyraźny sposób domniemań określonych w ust. 2 niniejszego artykułu, może odrzucić te argumenty w terminie, o którym mowa w ust. 4, bez stosowania procedury ustanowionej w art. 17 ust. 3.

W przypadku gdy przedsiębiorstwo świadczące podstawowe usługi platformowe przedstawi takie dostatecznie uzasadnione argumenty podważające w wyraźny sposób domniemania określone w ust. 2 niniejszego artykułu, Komisja może – niezależnie od akapitu pierwszego niniejszego ustępu – wszcząć procedurę ustanowioną w art. 17 ust. 3 w terminie, o którym mowa w ust. 4 niniejszego artykułu.

Jeżeli Komisja stwierdzi, że przedsiębiorstwo świadczące podstawowe usługi platformowe nie było w stanie wykazać, że świadczona przez nie odpowiednia podstawowa usługa platformowa nie spełnia wymogów wymienionych w ust. 1 niniejszego artykułu, wskazuje to przedsiębiorstwo jako strażnika dostępu zgodnie z procedurą ustanowioną w art. 17 ust. 3.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 49 w celu uzupełniania niniejszego rozporządzenia poprzez doprecyzowanie metodyki ustalania, czy osiągnięte zostały progi ilościowe ustanowione w ust. 2 niniejszego artykułu, oraz – w razie potrzeby – w celu regularnego dostosowywania tej metodyki do zmian na rynku i rozwoju technologicznego.

7. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 49 w celu zmiany niniejszego rozporządzenia poprzez aktualizację metodyki i wykazu wskaźników określonych w załączniku.

8. Zgodnie z procedurą ustanowioną w art. 17 Komisja wskazuje jako strażnika dostępu dowolne przedsiębiorstwo świadczące podstawowe usługi platformowe, które osiągnęło wszystkie wymogi wymienione w ust. 1 niniejszego artykułu, ale które nie osiągnęło wszystkich progów ustanowionych w ust. 2 niniejszego artykułu.

W tym celu Komisja bierze pod uwagę niektóre lub wszystkie następujące elementy, w zakresie, w jakim są one istotne dla danego przedsiębiorstwa świadczącego podstawowe usługi platformowe:

- a) wielkość, w tym obrót i kapitalizację rynkową, działalność prowadzoną przez to przedsiębiorstwo oraz jego pozycję;
- b) liczbę użytkowników biznesowych korzystających z podstawowej usługi platformowej w celu docierania do użytkowników końcowych oraz liczbę użytkowników końcowych;

- c) efekty sieciowe i korzyści wynikające z dostępu do danych, w szczególności w odniesieniu do dostępu tego przedsiębiorstwa do danych osobowych i nieosobowych oraz zbierania przez nie takich danych lub jego zdolności analitycznych;
- d) korzyści skali i zakresu odnoszone przez przedsiębiorstwo, w tym pod względem danych oraz, w stosownych przypadkach, jego działalności poza Unią;
- e) uzależnienie użytkowników biznesowych i użytkowników końcowych od jednego dostawcy, w tym koszty zmiany i mechanizmy behawioralne ograniczające zdolność użytkowników biznesowych i użytkowników końcowych do zmiany lub do korzystania z wielu platform („multi-homing”);
- f) struktura korporacyjna mająca formę konglomeratu lub struktura zintegrowana pionowo tego przedsiębiorstwa, na przykład umożliwiającą mu subsydiowanie skrośne, łączenie danych pochodzących z różnych źródeł lub wykorzystywanie swojej pozycji; lub
- g) inne strukturalne cechy działalności lub usług.

Przeprowadzając ocenę na podstawie niniejszego ustępu, Komisja bierze pod uwagę możliwe do przewidzenia zmiany dotyczące elementów wymienionych w akapicie drugim, w tym planowane koncentracje z udziałem innego przedsiębiorstwa świadczącego podstawowe usługi platformowe lub świadczącego dowolne inne usługi w sektorze cyfrowym lub umożliwiającego zbieranie danych.

W przypadku gdy przedsiębiorstwo świadczące podstawową usługę platformową, które nie osiągnęło progów ilościowych ustanowionych w ust. 2, nie zastosuje się w znacznym stopniu do środków zarządzanych przez Komisję w ramach badania, pomimo wezwania do zastosowania się do tych czynności w rozsądnym terminie i do przedstawienia uwag, Komisja może wskazać to przedsiębiorstwo jako strażnika dostępu na podstawie faktów, którymi dysponuje.

9. W przypadku każdego przedsiębiorstwa wskazanego jako strażnik dostępu na podstawie ust. 4 lub 8 Komisja zamieszcza w decyzji o wskazaniu wykaz odpowiednich podstawowych usług platformowych świadczonych w ramach tego przedsiębiorstwa, z których każda indywidualnie stanowi ważny punkt dostępu dla użytkowników biznesowych, za pośrednictwem którego docierają oni zgodnie z ust. 1 lit. b) do użytkowników końcowych.

10. Strażnik dostępu jest zobowiązany wypełnić obowiązki ustanowione w art. 5, 6 i 7 w terminie 6 miesięcy od dnia, w którym podstawowa usługa platformowa została wymieniona w decyzji o wskazaniu zgodnie z ust. 9 niniejszego artykułu.

#### Artykuł 4

##### Przegląd statusu strażnika dostępu

1. Komisja może w dowolnym momencie, na wniosek lub z własnej inicjatywy, ponownie rozpatrzyć, zmienić lub uchylić przyjętą na podstawie art. 3 decyzję o wskazaniu z jednego z następujących powodów:

- a) nastąpiła istotna zmiana stanu faktycznego, na podstawie którego podjęta została decyzja o wskazaniu;
- b) decyzja o wskazaniu została podjęta na podstawie niekompletnych, nieprawdziwych lub wprowadzających w błąd informacji.

2. Komisja regularnie, przynajmniej raz na 3 lata, dokonuje przeglądu służącego ustaleniu, czy strażnicy dostępu nadal spełniają wymogi ustanowione w art. 3 ust. 1. W ramach tego przeglądu bada się również konieczność zmiany wykazu podstawowych usług platformowych strażników dostępu, z których każda indywidualnie stanowi ważny punkt dostępu dla użytkowników biznesowych, za pośrednictwem którego docierają oni zgodnie z art. 3 ust. 1 lit. b) do użytkowników końcowych. Przeglądy te nie mają skutku zawieszającego w odniesieniu do obowiązków strażnika dostępu.

Komisja sprawdza również, przynajmniej co roku, czy nowe przedsiębiorstwa świadczące podstawowe usługi platformowe spełniają te wymogi.



Jeżeli po przeprowadzeniu przeglądu na podstawie akapitu pierwszego Komisja stwierdzi, że zmienił się stan faktyczny, na podstawie którego przedsiębiorstwa świadczące podstawowe usługi platformowe zostały wskazane jako strażnicy dostępu, przyjmuje decyzję potwierdzającą, zmieniającą lub uchylającą decyzję o wskazaniu.

3. Komisja publikuje i aktualizuje na bieżąco wykaz strażników dostępu oraz wykaz podstawowych usług platformowych, w odniesieniu do których muszą oni wypełniać obowiązki ustanowione w rozdziale III.

## ROZDZIAŁ III

### PRAKTYKI STRAŻNIKÓW DOSTĘPU, KTÓRE OGRANICZAJĄ KONTESTOWALNOŚĆ LUB SĄ NIEUCZCIWE

#### Artykuł 5

#### Obowiązki strażników dostępu

1. Strażnik dostępu jest zobowiązany do wypełniania wszystkich obowiązków określonych w niniejszym artykule w odniesieniu do każdej z podstawowych usług platformowych wymienionych w decyzji o wskazaniu na podstawie art. 3 ust. 9.

2. Strażnik dostępu nie może dokonywać żadnej z poniższych czynności:

- a) przetwarzać – do celów świadczenia internetowych usług reklamowych – danych osobowych użytkowników końcowych, którzy korzystają ze świadczonych przez osoby trzecie usług wykorzystujących podstawowe usługi platformowe strażnika dostępu;
- b) łączyć danych osobowych pochodzących z danej podstawowej usługi platformowej z danymi osobowymi pochodzącymi z innych podstawowych usług platformowych lub z dowolnych innych usług świadczonych przez strażnika dostępu lub z danymi osobowymi pochodzącymi z usług świadczonych przez osoby trzecie;
- c) wykorzystywać danych osobowych pochodzących z danej podstawowej usługi platformowej w ramach innych usług świadczonych oddzielnie przez strażnika dostępu, w tym innych podstawowych usług platformowych, i odwrotnie – wykorzystywać danych osobowych pochodzących z takich innych usług w ramach podstawowej usługi platformowej; oraz
- d) logować użytkowników końcowych do innych usług świadczonych przez strażnika dostępu, po to by łączyć dane osobowe,

chyba że użytkownikowi końcowemu zapewniono możliwość dokonania konkretnego wyboru i wyraził on zgodę w rozumieniu art. 4 pkt 11 i art. 7 rozporządzenia (UE) 2016/679.

W przypadku gdy użytkownik końcowy odmówił wyrażenia zgody do celu akapitu pierwszego lub cofnął taką zgodę, strażnik dostępu nie może występować z ponownym wnioskiem o wyrażenie zgody do tego samego celu częściej niż raz w ciągu rocznego okresu.

Niniejszy ustęp pozostaje bez uszczerbku dla możliwości powołania się przez strażnika dostępu w stosownych przypadkach na art. 6 ust. 1 lit. c), d) i e) rozporządzenia (UE) 2016/679.

3. Strażnik dostępu nie może uniemożliwiać użytkownikom biznesowym oferowania, przy wykorzystaniu usług pośrednictwa internetowego świadczonych przez osobę trzecią lub za pomocą własnych kanałów bezpośredniej sprzedaży internetowej, tych samych produktów lub usług użytkownikom końcowym po cenach lub na warunkach innych niż w ramach usług pośrednictwa internetowego świadczonych przez strażnika dostępu.

4. Strażnik dostępu zezwala nieodpłatnie użytkownikom biznesowym na przedstawianie ofert, w tym ofert na innych warunkach, użytkownikom końcowym pozyskanym za pośrednictwem jego podstawowej usługi platformowej lub za pośrednictwem innych kanałów oraz promowania takich ofert wśród tych użytkowników końcowych oraz na zawieranie z tymi użytkownikami końcowymi umów niezależnie od tego, czy korzystają oni w tym celu z podstawowych usług platformowych świadczonych przez strażnika dostępu.

5. Strażnik dostępu zezwala użytkownikom końcowym na dostęp i korzystanie, za pośrednictwem jego podstawowych usług platformowych, z treści, subskrypcji, funkcji lub innych elementów – przy użyciu aplikacji użytkownika biznesowego, w tym w przypadku gdy ci użytkownicy końcowi nabyli takie elementy od danego użytkownika biznesowego bez korzystania z podstawowych usług platformowych strażnika dostępu.

6. Strażnik dostępu nie może uniemożliwiać ani utrudniać – bezpośrednio lub pośrednio – użytkownikom biznesowym lub użytkownikom końcowym dokonywania zgłoszeń do odpowiednich organów publicznych, w tym sądów krajowych, dotyczących nieprzestrzegania przez strażnika dostępu odpowiednich przepisów prawa Unii lub prawa krajowego w odniesieniu do stosowanych przez strażnika dostępu praktyk. Pozostaje to bez uszczerbku dla prawa użytkowników biznesowych i strażników dostępu do określenia w swoich umowach warunków korzystania z dozwolonych prawem mechanizmów rozpatrywania skarg.

7. Strażnik dostępu nie może nakładać na użytkowników końcowych obowiązku korzystania z usługi identyfikacyjnej, silnika przeglądarki internetowej, usługi płatniczej lub usług technicznych wspierających świadczenie usług płatniczych, takich jak systemy płatności za zakupy wewnątrz aplikacji, tego strażnika dostępu w ramach usług świadczonych przez użytkowników biznesowych z wykorzystaniem podstawowych usług platformowych tego strażnika dostępu lub – w odniesieniu do użytkowników biznesowych – obowiązku korzystania z takich usług, oferowania takich usług lub zapewnienia interoperacyjności z takimi usługami.

8. Strażnik dostępu nie może nakładać na użytkowników biznesowych lub użytkowników końcowych obowiązku subskrypcji lub zarejestrowania się jako użytkownik innych podstawowych usług platformowych wymienionych w decyzji o wskazaniu na podstawie art. 3 ust. 9 lub osiągających progi ustanowione w art. 3 ust. 2 lit. b) jako warunku, którego spełnienie umożliwia korzystanie z podstawowych usług platformowych tego strażnika dostępu wymienionych na podstawie tego artykułu, uzyskanie dostępu do tych usług, zapisanie się lub zarejestrowanie do tych usług.

9. Strażnik dostępu udziela codziennie i nieodpłatnie każdemu reklamodawcy, na rzecz którego świadczy internetowe usługi reklamowe, lub osobom trzecim upoważnionym przez reklamodawców, na wniosek danego reklamodawcy, informacji w odniesieniu do każdej reklamy umieszczanej przez reklamodawcę, które dotyczą:

- a) ceny zapłaconej przez tego reklamodawcę i pobranych od niego opłat, z uwzględnieniem wszelkich potrąceń i dodatkowych opłat, z tytułu każdej odpowiedniej internetowej usługi reklamowej świadczonej przez strażnika dostępu;
- b) wynagrodzenia otrzymanego przez wydawcę, z uwzględnieniem wszelkich potrąceń i dodatkowych opłat, z zastrzeżeniem zgody wydawcy; oraz
- c) mierników, na podstawie których obliczane są poszczególne ceny, opłaty i wynagrodzenia.

W przypadku gdy wydawca nie wyraża zgody na udostępnienie informacji dotyczących otrzymanego wynagrodzenia, o których mowa w akapicie pierwszym lit. b), strażnik dostępu udziela nieodpłatnie każdemu reklamodawcy informacji dotyczących średniego dziennego wynagrodzenia otrzymywanego przez tego wydawcę, z uwzględnieniem wszelkich potrąceń i dodatkowych opłat, z tytułu odpowiednich reklam.

10. Strażnik dostępu udziela codziennie i nieodpłatnie każdemu wydawcy, na rzecz którego świadczy internetowe usługi reklamowe, lub osobom trzecim upoważnionym przez wydawców, na wniosek danego wydawcy, informacji w odniesieniu do każdej reklamy wyświetlanej w ramach zasobów wydawcy, które dotyczą:

- a) wynagrodzenia otrzymanego przez tego wydawcę i pobranych od niego opłat, z uwzględnieniem wszelkich potrąceń i dodatkowych opłat, z tytułu każdej odpowiedniej internetowej usługi reklamowej świadczonej przez strażnika dostępu;
- b) ceny zapłaconej przez reklamodawcę, z uwzględnieniem wszelkich potrąceń i dodatkowych opłat, z zastrzeżeniem zgody reklamodawcy; oraz
- c) mierników, na podstawie których obliczane są poszczególne ceny i wynagrodzenia.

W przypadku gdy reklamodawca nie wyraża zgody na udostępnienie informacji strażnik dostępu udziela nieodpłatnie każdemu wydawcy informacji dotyczących średniej dziennej ceny płaconej przez tego reklamodawcę, z uwzględnieniem wszelkich potrąceń i dodatkowych opłat, z tytułu odpowiednich reklam.

#### Artykuł 6

### **Obowiązki strażników dostępu, które mogą podlegać doprecyzowaniu na podstawie art. 8**

1. Strażnik dostępu jest zobowiązany do wypełniania wszystkich obowiązków określonych w niniejszym artykule w odniesieniu do każdej z podstawowych usług platformowych wymienionych w decyzji o wskazaniu na podstawie art. 3 ust. 9.

2. Strażnik dostępu nie może wykorzystywać – konkurując z użytkownikami biznesowymi – niedostępnych publicznie danych wygenerowanych lub dostarczonych przez tych użytkowników biznesowych w ramach korzystania przez nich z odpowiednich podstawowych usług platformowych lub usług świadczonych wraz z odpowiednimi podstawowymi usługami platformowymi lub wspierających takie usługi, w tym danych wygenerowanych lub dostarczonych przez klientów tych użytkowników biznesowych.

Do celów akapitu pierwszego niedostępne publicznie dane obejmują wszelkie zagregowane i niezagregowane dane wygenerowane przez użytkowników biznesowych w ramach odpowiednich podstawowych usług platformowych lub usług świadczonych wraz z odpowiednimi podstawowymi usługami platformowymi lub wspierających takie usługi, które to dane można wyprowadzić z działalności handlowej użytkowników biznesowych lub ich klientów lub zebrać w toku takiej działalności, w tym dane dotyczące kliknięć, zapytań, wyświetleń i dane głosowe.

3. Strażnik dostępu umożliwia użytkownikom końcowym – także pod względem technicznym – łatwe odinstalowanie wszelkich aplikacji w systemie operacyjnym strażnika dostępu, bez uszczerbku dla możliwości ograniczenia przez tego strażnika dostępu takiego odinstalowania w odniesieniu do aplikacji mających kluczowe znaczenie dla funkcjonowania danego systemu operacyjnego lub urządzenia, w przypadku gdy aplikacje te nie mogą być oferowane – ze względów technicznych – przez osoby trzecie jako autonomiczny produkt.

Strażnik dostępu umożliwia użytkownikom końcowym – także pod względem technicznym – łatwą zmianę w systemie operacyjnym, wirtualnym asystencie i przeglądarce internetowej strażnika dostępu ustawień domyślnych, które kierują użytkowników końcowych do produktów dostarczanych lub usług świadczonych przez strażnika dostępu lub naprowadzają ich na takie produkty lub usługi. Obejmuje to skłanianie użytkowników końcowych, w momencie korzystania przez nich po raz pierwszy z wyszukiwarki internetowej, wirtualnego asystenta lub przeglądarki internetowej strażnika dostępu wymienionych w decyzji o wskazaniu na podstawie art. 3 ust. 9, aby z listy głównych dostępnych usługodawców wybrali wyszukiwarkę internetową, wirtualnego asystenta lub przeglądarkę internetową, do których system operacyjny strażnika dostępu domyślnie kieruje użytkowników lub na które ich domyślnie naprowadza, oraz wyszukiwarkę internetową, do której wirtualny asystent i przeglądarka internetowa strażnika dostępu domyślnie kierują użytkowników lub na które ich domyślnie naprowadzają.

4. Strażnik dostępu umożliwia – także pod względem technicznym – instalację i skuteczne korzystanie z oferowanych przez osoby trzecie aplikacji lub sklepów z aplikacjami korzystających z jego systemu operacyjnego lub współpracujących z jego systemem operacyjnym oraz zapewnia możliwość uzyskania dostępu do tych aplikacji lub sklepów z aplikacjami w inny sposób niż za pośrednictwem odpowiednich podstawowych usług platformowych tego strażnika dostępu. W stosownych przypadkach strażnik dostępu nie może uniemożliwiać skłaniania użytkowników końcowych przez pobrane aplikacje lub pobrane sklepy z aplikacjami oferowane przez osoby trzecie, by zdecydowali oni, czy chcą ustawić pobraną aplikację lub pobrany sklep z aplikacjami jako domyślne. Strażnik dostępu umożliwia użytkownikom końcowym, którzy zdecydują się na ustawienie pobranej aplikacji lub pobranego sklepu z aplikacjami jako domyślnych, łatwe dokonanie tej zmiany pod względem technicznym.

Nie zabrania się strażnikowi dostępu podejmowania działań, w zakresie bezwzględnie koniecznym i proporcjonalnym, w celu zapewnienia, aby aplikacje lub sklepy z aplikacjami oferowane przez osoby trzecie nie zagrażały integralności dostarczanego przez strażnika dostępu sprzętu lub systemu operacyjnego, pod warunkiem że takie działania są należycie uzasadnione przez strażnika dostępu.

Ponadto nie zabrania się strażnikowi dostępu stosowania, w zakresie bezwzględnie koniecznym i proporcjonalnym, środków i ustawień innych niż ustawienia domyślne, umożliwiających użytkownikom końcowym skuteczną ochronę bezpieczeństwa w odniesieniu do aplikacji lub sklepów z aplikacjami oferowanych przez osoby trzecie, pod warunkiem że takie środki i ustawienia inne niż ustawienia domyślne są należycie uzasadnione przez strażnika dostępu.

5. Strażnik dostępu nie może traktować – w ramach plasowania oraz związanego z nim indeksowania i badania (crawlingu) – usług i produktów oferowanych przez samego strażnika dostępu na korzystniejszych zasadach niż podobne usługi lub produkty oferowane przez osobę trzecią. Strażnik dostępu dokonuje takiego plasowania na przejrzystych, sprawiedliwych i niedyskryminujących warunkach.

6. Strażnik dostępu nie może ograniczać – pod względem technicznym lub w inny sposób – możliwości korzystania przez użytkowników końcowych z różnych aplikacji i usług, do których uzyskuje się dostęp przy użyciu podstawowych usług platformowych strażnika dostępu, oraz możliwości subskrypcji takich różnych aplikacji i usług, w tym również w zakresie wyboru usług dostępu do internetu przez użytkowników końcowych;

7. Strażnik dostępu umożliwia nieodpłatnie dostawcom usług i dostawcom sprzętu skuteczną interoperacyjność z tymi samymi funkcjami sprzętu i oprogramowania jakimi dysponują usługi świadczone lub sprzęt dostarczany przez strażnika dostępu, do których to funkcji uzyskuje się dostęp lub które to funkcje są kontrolowane za pośrednictwem systemu operacyjnego lub wirtualnego asystenta wymienionych w decyzji o wskazaniu na podstawie art. 3 ust. 9, a także umożliwia tym dostawcom dostęp do tych funkcji do celów interoperacyjności. Strażnik dostępu umożliwia ponadto nieodpłatnie użytkownikom biznesowym i alternatywnym dostawcom usług świadczonych wraz z odpowiednimi podstawowymi usługami platformowymi lub wspierających takie usługi skuteczną interoperacyjność z tym samym systemem operacyjnym i tymi samymi funkcjami sprzętu i oprogramowania – niezależnie od tego, czy funkcje te są częścią systemu operacyjnego – jakimi dysponuje lub z których korzysta ten strażnik dostępu, świadcząc takie usługi, a także umożliwia tym użytkownikom i dostawcom dostęp do tego systemu i do tych funkcji do celów interoperacyjności.

Nie zabrania się strażnikowi dostępu podejmowania bezwzględnie koniecznych i proporcjonalnych działań w celu zapewnienia, aby interoperacyjność nie zagrażała integralności systemu operacyjnego, wirtualnego asystenta, funkcji sprzętu lub oprogramowania dostarczanych przez strażnika dostępu, pod warunkiem że takie działania są przez strażnika dostępu należycie uzasadnione.

8. Strażnik dostępu zapewnia nieodpłatnie reklamodawcom i wydawcom, a także osobom trzecim upoważnionym przez reklamodawców i wydawców – na ich wniosek – dostęp do stosowanych przez strażnika dostępu narzędzi pomiaru wyników oraz do danych potrzebnych reklamodawcom i wydawcom do przeprowadzenia samodzielnie niezależnej weryfikacji zasobów reklamowych, w tym do danych zagregowanych i niezagregowanych. Dane takie podawane są w sposób umożliwiający reklamodawcom i wydawcom wykorzystanie ich własnych narzędzi weryfikacyjnych i pomiarowych do oceny wyników podstawowych usług platformowych świadczonych przez strażników dostępu.

9. Strażnik dostępu zapewnia nieodpłatnie użytkownikom końcowym i osobom trzecim upoważnionym przez użytkownika końcowego – na ich wniosek – skuteczną możliwość przenoszenia danych dostarczonych przez użytkownika końcowego lub wygenerowanych w toku działalności użytkownika końcowego w ramach korzystania z odpowiedniej podstawowej usługi platformowej, między innymi zapewniając nieodpłatnie narzędzia ułatwiające skuteczne korzystanie z takiej możliwości przenoszenia danych, w tym poprzez zapewnianie stałej możliwości uzyskania dostępu do takich danych w czasie rzeczywistym.

10. Strażnik dostępu zapewnia nieodpłatnie użytkownikom biznesowym i osobom trzecim upoważnionym przez użytkownika biznesowego – na ich wniosek – skuteczny, wysokiej jakości i stały dostęp w czasie rzeczywistym do danych zagregowanych i niezagregowanych, w tym do danych osobowych, oraz możliwość korzystania z tych danych, dostarczanych lub generowanych w ramach korzystania – przez tych użytkowników biznesowych oraz przez użytkowników końcowych korzystających z produktów dostarczanych lub usług świadczonych przez tych użytkowników biznesowych – z odpowiednich podstawowych usług platformowych lub usług świadczonych wraz z odpowiednimi podstawowymi usługami platformowymi lub wspierających takie usługi. W odniesieniu do danych osobowych strażnik dostępu zapewnia taki dostęp do danych i możliwość korzystania z nich wyłącznie wówczas, gdy dane są bezpośrednio powiązane z faktem korzystania przez użytkowników końcowych z produktów lub usług oferowanych przez odpowiedniego użytkownika biznesowego za pośrednictwem odpowiedniej podstawowej usługi platformowej oraz gdy użytkownicy końcowi zdecydują się udostępnić takie dane, wyrażając na to zgodę.

11. Strażnik dostępu zapewnia przedsiębiorstwu będącemu dostawcą wyszukiwarek internetowych, które jest osobą trzecią, na jego wniosek, dostęp, na sprawiedliwych, rozsądnych i niedyskryminujących warunkach, do danych dotyczących plasowania, zapytań, kliknięć i wyświetleń związanych z nieodpłatnym i płatnym wyszukiwaniem, wygenerowanych przez użytkowników końcowych przy wykorzystaniu jego wyszukiwarek internetowych. Wszelkie takie dane dotyczące zapytań, kliknięć i wyświetleń będące danymi osobowymi poddaje się anonimizacji.

12. Strażnik dostępu stosuje sprawiedliwe, rozsądne i niedyskryminujące ogólne warunki dostępu użytkowników biznesowych do swoich sklepów z aplikacjami, wyszukiwarek internetowych i internetowych serwisów społecznościowych wymienionych w decyzji o wskazaniu na podstawie art. 3 ust. 9.

W tym celu strażnik dostępu publikuje ogólne warunki dostępu, w tym dotyczące alternatywnego mechanizmu rozstrzygnięcia sporów.

Komisja ocenia, czy opublikowane ogólne warunki dostępu są zgodne z niniejszym ustępem.

13. Strażnik dostępu nie ustanawia nieproporcjonalnych ogólnych warunków rezygnacji z podstawowej usługi platformowej. Strażnik dostępu zapewnia korzystanie z warunków rezygnacji bez zbędnych trudności.

## Artykuł 7

**Obowiązki strażników dostępu dotyczące interoperacyjności usług łączności interpersonalnej niewykorzystujących numerów**

1. W przypadku gdy strażnik dostępu świadczy usługi łączności interpersonalnej niewykorzystujące numerów wymienione w decyzji o wskazaniu na podstawie art. 3 ust. 9 zapewnia on interoperacyjność podstawowych funkcjonalności swoich usług łączności interpersonalnej niewykorzystujących numerów z tego rodzaju usługami świadczonymi przez innego dostawcę oferującego lub zamierzającego oferować takie usługi w Unii, dostarczając nieodpłatnie, na wniosek, niezbędne interfejsy techniczne lub podobne rozwiązania ułatwiające interoperacyjność.
2. W przypadku gdy strażnik dostępu sam dostarcza swoim własnym użytkownikom końcowym podstawowe funkcjonalności, o których mowa w ust. 1, zapewnia interoperacyjność co najmniej następujących funkcjonalności:
  - a) po wymienieniu przedmiotowych usług w decyzji o wskazaniu na podstawie art. 3 ust. 9:
    - (i) przesyłania wiadomości tekstowych metodą „od końca do końca” („end-to-end”) między dwoma pojedynczymi użytkownikami końcowymi;
    - (ii) udostępniania obrazów, wiadomości głosowych, wideo i innych załączonych plików w ramach komunikacji metodą „od końca do końca” między dwoma pojedynczymi użytkownikami końcowymi;
  - b) w terminie 2 lat od wskazania:
    - (i) przesyłania wiadomości tekstowych metodą „od końca do końca” w obrębie grup pojedynczych użytkowników końcowych;
    - (ii) udostępniania obrazów, wiadomości głosowych, wideo i innych załączonych plików w ramach komunikacji metodą „od końca do końca” między czatem grupowym a pojedynczym użytkownikiem końcowym;
  - c) w terminie 4 lat od wskazania:
    - (i) połączeń głosowych metodą „od końca do końca” między dwoma pojedynczymi użytkownikami końcowymi;
    - (ii) połączeń wideo metodą „od końca do końca” między dwoma pojedynczymi użytkownikami końcowymi;
    - (iii) połączeń głosowych metodą „od końca do końca” między czatem grupowym a pojedynczym użytkownikiem końcowym;
    - (iv) połączeń wideo metodą „od końca do końca” między czatem grupowym a pojedynczym użytkownikiem końcowym.
3. Poziom bezpieczeństwa, w tym, w stosownych przypadkach, szyfrowanie „od końca do końca”, zapewniany przez strażnika dostępu swoim własnym użytkownikom końcowym zostaje zachowany w odniesieniu do wszystkich interoperacyjnych usług.
4. Strażnik dostępu publikuje ofertę ramową określającą szczegółowe informacje techniczne oraz ogólne warunki interoperacyjności ze świadczonymi przez niego usługami łączności interpersonalnej niewykorzystującymi numerów, w tym niezbędne szczegółowe informacje dotyczące poziomu bezpieczeństwa oraz szyfrowania „od końca do końca”. Strażnik dostępu publikuje tę ofertę ramową w terminie określonym w art. 3 ust. 10 i w razie potrzeby ją aktualizuje.
5. Po opublikowaniu oferty ramowej zgodnie z ust. 4, każdy dostawca usług łączności interpersonalnej niewykorzystujących numerów oferujący lub zamierzający oferować takie usługi w Unii może wystąpić z wnioskiem o zapewnienie interoperacyjności z usługami łączności interpersonalnej niewykorzystującymi numerów świadczonymi przez strażnika dostępu. Taki wniosek może obejmować niektóre lub wszystkie podstawowe funkcjonalności wymienione w ust. 2. Strażnik dostępu uwzględni każdy zasadny wniosek o zapewnienie interoperacyjności w terminie 3 miesięcy od otrzymania takiego wniosku poprzez zapewnienie działania podstawowych funkcjonalności będących przedmiotem wniosku.
6. Komisja może, na zasadzie wyjątku i na uzasadniony wniosek strażnika dostępu, przedłużyć terminy na wypełnienie obowiązków określonych w ust. 2 lub 5, w przypadku gdy strażnik dostępu wykaże, że jest to niezbędne w celu zapewnienia skutecznej interoperacyjności oraz zachowania niezbędnego poziomu bezpieczeństwa, w tym, w stosownych przypadkach, szyfrowania „od końca do końca”.

7. Użytkownicy końcowi usług łączności interpersonalnej niewykorzystujących numerów świadczonych przez strażnika końcowego oraz użytkownicy końcowi dostawcy takich usług występującego z wnioskiem zachowują swobodę wyboru co do korzystania z interoperacyjnych podstawowych funkcjonalności, które może zapewniać strażnik dostępu na podstawie ust. 1.

8. Strażnik dostępu zbiera i wymienia z dostawcą usług łączności interpersonalnej niewykorzystujących numerów występującym z wnioskiem o zapewnienie interoperacyjności wyłącznie te dane osobowe użytkowników końcowych, które są bezwzględnie konieczne do zapewnienia skutecznej interoperacyjności. Takie zbieranie i wymiana danych osobowych użytkowników końcowych muszą być w pełni zgodne z rozporządzeniem (UE) 2016/679 i dyrektywą 2002/58/WE.

9. Nie zabrania się strażnikowi dostępu podejmowania działań w celu zapewnienia, by osoby trzecie będące dostawcami usług łączności interpersonalnej niewykorzystujących numerów, które wystąpią z wnioskiem o zapewnienie interoperacyjności, nie stanowiły zagrożenia dla integralności, bezpieczeństwa i ochrony prywatności w ramach jego usług, pod warunkiem że takie działania są bezwzględnie konieczne i proporcjonalne, oraz że są należycie uzasadnione przez strażnika dostępu.

## Artykuł 8

### Wypełnianie obowiązków strażników dostępu

1. Strażnik dostępu zapewnia wypełnianie obowiązków ustanowionych w art. 5, 6 i 7 niniejszego rozporządzenia i wykazuje ich wypełnianie. Środki, jakie strażnik dostępu wdraża, aby zapewnić przestrzeganie tych artykułów, muszą skutecznie przyczynić się do osiągnięcia celów niniejszego rozporządzenia i celu, w jakim ustanowiono dany obowiązek. Strażnik dostępu zapewnia, by wdrożenie tych środków było zgodne z mającym zastosowanie prawem, w szczególności z rozporządzeniem (UE) 2016/679, dyrektywą 2002/58/WE, przepisami w zakresie cyberbezpieczeństwa, ochrony konsumentów i bezpieczeństwa produktów, a także z wymogami dostępności.

2. Komisja może – z własnej inicjatywy lub na wniosek strażnika dostępu na podstawie ust. 3 niniejszego artykułu – wszcząć postępowanie na podstawie art. 20.

Komisja może przyjąć akt wykonawczy określający środki, które dany strażnik dostępu ma wdrożyć w celu skutecznego wypełnienia obowiązków ustanowionych w art. 6 i 7. Akt wykonawczy przyjmuje się w terminie 6 miesięcy od dnia wszczęcia postępowania na podstawie art. 20 zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.

W przypadku wszczęcia przez Komisję postępowania z własnej inicjatywy w przypadku obchodzenia obowiązków, na podstawie art. 13, takie środki mogą dotyczyć obowiązków ustanowionych w art. 5, 6 i 7.

3. Strażnik dostępu może zwrócić się do Komisji z wnioskiem o wszczęcie postępowania w celu ustalenia, czy środki, jakie strażnik dostępu zamierza wdrożyć lub wdrożył, by zapewnić przestrzeganie art. 6 i 7, skutecznie przyczyniają się w określonej sytuacji tego strażnika dostępu do osiągnięcia celu, w jakim ustanowiono dany obowiązek. Komisja ma swobodę decydowania, czy wszcząć takie postępowanie, z poszanowaniem zasad równego traktowania, proporcjonalności i dobrej administracji.

Strażnik dostępu przedstawia w swoim wniosku uzasadnioną opinię zawierającą wyjaśnienie środków, które zamierza wdrożyć lub wdrożył. Strażnik dostępu przedstawia ponadto jawną wersję swojej uzasadnionej opinii, którą można udostępnić osobom trzecim na podstawie ust. 6.

4. Ust. 2 i 3 niniejszego artykułu pozostają bez uszczerbku dla uprawnień przyznanych Komisji na mocy art. 29, 30 i 31.

5. W celu przyjęcia decyzji na podstawie ust. 2 Komisja przekazuje strażnikowi dostępu swoje wstępne ustalenia w terminie 3 miesięcy od dnia wszczęcia postępowania na podstawie art. 20. We wstępnych ustaleniach Komisja wyjaśnia środki, których wprowadzenie rozważa lub które jej zdaniem dany strażnik dostępu powinien wprowadzić w celu skutecznego zastosowania się do wstępnych ustaleń.

6. Aby umożliwić zainteresowanym osobom trzecim skuteczne zgłaszanie uwag, Komisja w momencie przekazywania swoich wstępnych ustaleń strażnikowi dostępu na podstawie ust. 5 lub jak najszybciej po przekazaniu tych ustaleń publikuje jawne streszczenie zawierające opis danej sprawy i środków, których wprowadzenie rozważa lub które jej zdaniem dany strażnik dostępu powinien wprowadzić. Komisja określa rozsądny termin na zgłaszanie takich uwag.

7. Określając środki, o których mowa w ust. 2, Komisja zapewnia, aby skutecznie przyczyniały się one do osiągnięcia celów niniejszego rozporządzenia i celu, w jakim ustanowiono dany obowiązek, oraz były proporcjonalne w określonej sytuacji strażnika dostępu i odpowiedniej usługi.

8. Na potrzeby doprecyzowania obowiązków, o których mowa w art. 6 ust. 11 i 12, Komisja ocenia również, czy zamierzone lub wdrożone środki zapewniają wyeliminowanie braku równowagi między prawami i obowiązkami użytkowników biznesowych oraz czy środki te same w sobie nie zapewniają strażnikowi dostępu korzyści, które byłyby nieproporcjonalne względem usługi świadczonej przez niego na rzecz użytkowników biznesowych.

9. W odniesieniu do postępowania na podstawie ust. 2 Komisja może, na wniosek lub z własnej inicjatywy, zdecydować o wznowieniu postępowania, w przypadku gdy:

- a) nastąpiła istotna zmiana stanu faktycznego, na podstawie którego podjęta została decyzja; lub
- b) decyzja została podjęta na podstawie niekompletnych, nieprawdziwych lub wprowadzających w błąd informacji; lub
- c) środki doprecyzowane w decyzji nie są skuteczne.

#### Artykuł 9

#### Zawieszenie

1. W przypadku gdy strażnik dostępu wykaże w uzasadnionym wniosku, że wypełnienie określonego obowiązku ustanowionego w art. 5, 6 lub 7 w odniesieniu do podstawowej usługi platformowej wymienionej w decyzji o wskazaniu na podstawie art. 3 ust. 9 zagrażałoby – z uwagi na wystąpienie wyjątkowych okoliczności pozostających poza kontrolą strażnika dostępu – rentowności działalności prowadzonej przez niego w Unii, Komisja może przyjąć akt wykonawczy określający jej decyzję o zawieszeniu na zasadzie wyjątku, w całości lub w części, określonego obowiązku, o którym mowa w tym uzasadnionym wniosku (zwaną dalej „decyzją o zawieszeniu”). W akcie wykonawczym Komisja uzasadnia swoją decyzję o zawieszeniu, określając wyjątkowe okoliczności uzasadniające zawieszenie. Akt wykonawczy jest ograniczony – pod względem zakresu i czasu obowiązywania – do tego, co jest niezbędne w celu wyeliminowania takiego zagrożenia dla rentowności strażnika dostępu. Komisja dąży do przyjęcia aktu wykonawczego niezwłocznie, nie później niż 3 miesiące od dnia otrzymania kompletnego uzasadnionego wniosku. Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.

2. W przypadku przyznania zawieszenia na podstawie ust. 1 Komisja dokonuje co roku przeglądu decyzji o zawieszeniu, chyba że w danej decyzji określono krótszy termin. Po przeprowadzeniu takiego przeglądu Komisja uchyla zawieszenie w całości lub częściowo albo stwierdza, że warunki określone w ust. 1 pozostają spełnione.

3. W pilnych przypadkach Komisja może – działając na uzasadniony wniosek strażnika dostępu – tymczasowo zawiesić konieczność wypełniania określonego obowiązku, o którym mowa w ust. 1, w odniesieniu do jednej podstawowej usługi platformowej lub większej ich liczby jeszcze przed przyjęciem decyzji na podstawie tego ustępu. Taki wniosek może zostać złożony i uwzględniony w dowolnym momencie w trakcie rozpatrywania przez Komisję wniosku na podstawie ust. 1.

4. Rozpatrując wniosek, o którym mowa w ust. 1 i 3, Komisja bierze pod uwagę w szczególności wpływ wypełnienia określonego obowiązku na rentowność działalności strażnika dostępu w Unii, a także na osoby trzecie, w szczególności MŚP i konsumentów. Zawieszenie może podlegać warunkom i obowiązkom określonym przez Komisję, aby zapewnić sprawiedliwą równowagę między powyższymi interesami a celami niniejszego rozporządzenia.

### Artykuł 10

#### Zwolnienie ze względów zdrowia publicznego i bezpieczeństwa publicznego

1. Komisja może – na uzasadniony wniosek strażnika dostępu lub z własnej inicjatywy – przyjąć akt wykonawczy określający jej decyzję o zwolnieniu tego strażnika dostępu, w całości lub w części, z określonego obowiązku ustanowionego w art. 5, 6 lub 7 w odniesieniu do podstawowej usługi platformowej wymienionej w decyzji o wskazaniu na podstawie art. 3 ust. 9, jeżeli takie zwolnienie jest uzasadnione względami określonymi w ust. 3 niniejszego artykułu (zwaną dalej „decyzją o zwolnieniu”). Komisja przyjmuje decyzję o zwolnieniu w terminie 3 miesięcy od dnia otrzymania kompletnego uzasadnionego wniosku i przedstawia uzasadnienie wyjaśniające powody zwolnienia. Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.
2. W przypadku udzielenia zwolnienia na podstawie ust. 1 Komisja dokonuje przeglądu decyzji o zwolnieniu, w momencie gdy podstawa zwolnienia przestaje istnieć lub co najmniej raz w roku. Po przeprowadzeniu takiego przeglądu Komisja znosi zwolnienie w całości lub częściowo albo stwierdza, że warunki określone w ust. 1 pozostają spełnione.
3. Zwolnienia na podstawie ust. 1 można udzielić wyłącznie ze względów zdrowia publicznego lub bezpieczeństwa publicznego.
4. W pilnych przypadkach Komisja może – na uzasadniony wniosek strażnika dostępu lub z własnej inicjatywy – tymczasowo zawiesić konieczność wypełniania określonego obowiązku, o którym mowa w ust. 1, w odniesieniu do jednej podstawowej usługi platformowej lub większej ich liczby jeszcze przed przyjęciem decyzji na podstawie tego ustępu. Taki wniosek może zostać złożony i uwzględniony w dowolnym momencie w trakcie rozpatrywania przez Komisję wniosku na podstawie ust. 1.
5. Rozpatrując wniosek, o którym mowa w ust. 1 i 4, Komisja bierze pod uwagę w szczególności wpływ wypełniania określonego obowiązku na względy określone w ust. 3, a także na danego strażnika dostępu i na osoby trzecie. Komisja może określić warunki i obowiązki, którym podlega zawieszenie, aby zapewnić sprawiedliwą równowagę między założeniami leżącymi u podstaw względów określonych w ust. 3 a celami niniejszego rozporządzenia.

### Artykuł 11

#### Sprawozdawczość

1. W terminie 6 miesięcy od wskazania na podstawie art. 3 i zgodnie z art. 3 ust. 10 strażnik dostępu przekazuje Komisji sprawozdanie opisujące w szczególności i przejrzysty sposób środki, które wdrożył w celu wypełniania obowiązków ustanowionych w art. 5, 6 i 7.
2. W terminie, o którym mowa w ust. 1, strażnik dostępu publikuje i przekazuje Komisji jawne streszczenie tego sprawozdania.

Strażnik dostępu co najmniej raz w roku aktualizuje to sprawozdanie i jego jawne streszczenie.

Komisja udostępnia na swojej stronie internetowej link do tego jawnego streszczenia.

### Artykuł 12

#### Aktualizowanie obowiązków strażników dostępu

1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 49 w celu uzupełnienia niniejszego rozporządzenia w odniesieniu do obowiązków ustanowionych w art. 5 i 6. Te akty delegowane oparte są na badaniach rynku przeprowadzonych na podstawie art. 19, w ramach których stwierdzono konieczność aktualizacji tych obowiązków, by zaradzić praktykom, które ograniczają kontestowalność podstawowych usług platformowych lub są nieuczciwe w taki sam sposób jak praktyki, którym zaradzić mają obowiązki ustanowione w art. 5 i 6.



2. Zakres aktu delegowanego przyjętego zgodnie z ust. 1 jest ograniczony do:
- a) rozszerzenia obowiązku, stosowanego wyłącznie w odniesieniu do niektórych podstawowych usług platformowych, na inne podstawowe usługi platformowe wymienione w art. 2 pkt 2;
  - b) rozszerzenia obowiązku, który przynosi korzyści określonym użytkownikom biznesowym lub użytkownikom końcowym, tak by przynosił korzyści innym użytkownikom biznesowym lub użytkownikom końcowym;
  - c) określenia sposobu, w jaki mają być wypełniane przez strażników dostępu obowiązki ustanowione w art. 5 i 6 w celu zapewnienia skutecznego ich wypełniania;
  - d) rozszerzenia obowiązku, stosowanego wyłącznie w odniesieniu do niektórych usług świadczonych wraz z podstawowymi usługami platformowymi lub wspierających takie usługi, na inne usługi świadczone wraz z podstawowymi usługami platformowymi lub wspierające takie usługi;
  - e) rozszerzenia obowiązku, który ma zastosowanie wyłącznie w odniesieniu do niektórych rodzajów danych, na inne rodzaje danych;
  - f) dodania dalszych warunków, w przypadku gdy dany obowiązek nakłada określone warunki dotyczące postępowania strażnika dostępu; lub
  - g) zastosowania obowiązku regulującego relacje między kilkoma podstawowymi usługami platformowymi strażnika dostępu do relacji między daną podstawową usługą platformową a innymi usługami strażnika dostępu.
3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 49 w celu zmiany niniejszego rozporządzenia w odniesieniu do wykazu podstawowych funkcjonalności określonych w art. 7 ust. 2 poprzez dodanie lub usunięcie funkcjonalności w ramach usług łączności interpersonalnej niewykorzystujących numerów.

Te akty delegowane oparte są na badaniach rynku przeprowadzonych na podstawie art. 19, w ramach których stwierdzono konieczność aktualizacji tych obowiązków, by zaradzić praktykom, które ograniczają kontestowalność podstawowych usług platformowych lub są nieuczciwe w taki sam sposób jak praktyki, którym zaradzić mają obowiązki ustanowione w art. 7.

4. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 49 w celu uzupełnienia niniejszego rozporządzenia w odniesieniu do obowiązków ustanowionych w art. 7 poprzez określenie sposobu, w jaki mają być wypełniane przez strażników dostępu obowiązki ustanowione w art. 7 w celu zapewnienia skutecznego ich wypełniania. Te akty delegowane oparte są na badaniach rynku przeprowadzonych na podstawie art. 19, w ramach których stwierdzono konieczność aktualizacji tych obowiązków, by zaradzić praktykom, które ograniczają kontestowalność podstawowych usług platformowych lub są nieuczciwe w taki sam sposób jak praktyki, którym zaradzić mają obowiązki ustanowione w art. 7.

5. Praktykę, o której mowa w ust. 1, 3 i 4, uznaje się za ograniczającą kontestowalność podstawowych usług platformowych lub za nieuczciwą, jeżeli:

- a) praktyki tej dopuszczają się strażnicy dostępu i może ona utrudniać innowacje i ograniczać użytkownikom biznesowym i użytkownikom końcowym możliwości wyboru, ponieważ:
  - (i) trwale wpływa lub może trwale wpływać na kontestowalność podstawowej usługi platformowej lub innych usług w sektorze cyfrowym ze względu na tworzenie lub wzmacnianie barier wejścia dla innych przedsiębiorstw lub rozszerzania działalności w charakterze dostawcy podstawowej usługi platformowej lub innych usług w sektorze cyfrowym; lub
  - (ii) uniemożliwia innym podmiotom uzyskanie takiego samego dostępu do kluczowych zasobów, jakim dysponuje strażnik dostępu; lub
- b) zachodzi brak równowagi między prawami a obowiązkami użytkowników biznesowych, a strażnik dostępu uzyskuje od użytkowników biznesowych korzyści, które są nieproporcjonalne względem usługi świadczonej przez tego strażnika dostępu na rzecz tych użytkowników.

## Artykuł 13

**Przeciwdziałanie obchodzeniu obowiązków**

1. Przedsiębiorstwo świadczące podstawowe usługi platformowe nie może dokonywać segmentacji, podziału, dalszego podziału, fragmentacji lub rozdzielania tych usług za pomocą środków umownych, handlowych, technicznych lub innych środków w celu obejścia progów ilościowych określonych w art. 3 ust. 2. Tego rodzaju praktyki stosowane przez przedsiębiorstwo nie mogą uniemożliwiać Komisji wskazania takiego przedsiębiorstwa jako strażnika dostępu na podstawie art. 3 ust. 4.
2. Komisja może, jeżeli podejrzewa, że przedsiębiorstwo świadczące podstawowe usługi platformowe dopuszcza się praktyk określonych w ust. 1, zażądać od tego przedsiębiorstwa wszelkich informacji, które uzna za niezbędne do ustalenia, czy przedsiębiorstwo to dopuszcza się takich praktyk.
3. Strażnik dostępu zapewnia pełne i skuteczne wypełnianie obowiązków ustanowionych w art. 5, 6 i 7.
4. Strażnik dostępu nie może dopuszczać się zachowań, które w jakikolwiek sposób utrudniają skuteczne wypełnianie obowiązków ustanowionych w art. 5, 6 i 7, niezależnie od tego, czy zachowanie to ma charakter umowny, handlowy, techniczny lub jakikolwiek inny lub czy polega na stosowaniu technik behawioralnych lub projektowaniu interfejsu.
5. Jeżeli przestrzeganie niniejszego rozporządzenia wiąże się z koniecznością uzyskania zgody na zbieranie, przetwarzanie i udostępnianie danych osobowych oraz wykorzystywanie danych osobowych w ramach różnych usług, strażnik dostępu podejmuje konieczne działania, aby zapewnić użytkownikom biznesowym możliwość bezpośredniego uzyskania zgody na przetwarzanie tych danych w przypadkach, w których zgoda ta jest wymagana na mocy rozporządzenia (UE) 2016/679 lub dyrektywy 2002/58/WE, albo aby zapewnić przestrzeganie unijnych przepisów i zasad w zakresie ochrony danych i prywatności w inny sposób, w tym – w stosownych przypadkach – poprzez dostarczanie użytkownikom biznesowym należycie zanonimizowanych danych. Strażnik dostępu nie może doprowadzić do sytuacji, w której uzyskanie tej zgody przez użytkownika biznesowego będzie bardziej uciążliwe niż uzyskanie jej na potrzeby usług świadczonych przez samego strażnika dostępu.
6. Strażnik dostępu nie może pogarszać warunków ani obniżać jakości podstawowych usług platformowych świadczonych na rzecz użytkowników biznesowych lub użytkowników końcowych, którzy zdecydowali się skorzystać z praw lub możliwości wyboru ustanowionych w art. 5, 6 i 7, ani sprawiać, że korzystanie z tych praw lub możliwości będzie nadmiernie utrudnione, w tym poprzez oferowanie użytkownikom końcowym możliwości wyboru w sposób nieobiektywny, bądź też przez osłabianie autonomii, procesów decyzyjnych lub swobody wyboru użytkowników końcowych lub użytkowników biznesowych za pośrednictwem struktury, projektu, funkcji lub sposobu działania interfejsu użytkownika lub jego części.
7. W przypadku gdy strażnik dostępu obchodzi lub próbuje obchodzić którykolwiek z obowiązków określonych w art. 5, 6 lub 7 w jeden ze sposobów opisanych w ust. 4, 5 i 6 niniejszego artykułu, Komisja może wszcząć postępowanie na podstawie art. 20 i przyjąć akt wykonawczy, o którym mowa w art. 8 ust. 2, aby określić środki, które strażnik dostępu ma wdrożyć.
8. Ust. 6 niniejszego artykułu pozostaje bez uszczerbku dla uprawnień przyznanych Komisji na mocy art. 29, 30 i 31.

## Artykuł 14

**Obowiązek informowania o koncentracjach**

1. Strażnik dostępu informuje Komisję o każdej zamierzonej koncentracji w rozumieniu art. 3 rozporządzenia (WE) nr 139/2004 w przypadku gdy łączące się podmioty lub podmiot docelowy koncentracji świadczą podstawowe usługi platformowe lub inne usługi w sektorze cyfrowym lub umożliwiają zbieranie danych, niezależnie od tego, czy taka koncentracja podlega zgłoszeniu Komisji zgodnie z tym rozporządzeniem lub właściwemu krajowemu organowi ochrony konkurencji zgodnie z krajowymi przepisami dotyczącymi łączenia przedsiębiorstw.

Strażnik dostępu informuje Komisję o takiej koncentracji przed jej przeprowadzeniem i po zawarciu umowy, ogłoszeniu publicznej oferty przejęcia lub nabyciu kontrolnego pakietu akcji.

2. Informacje przekazane przez strażnika dostępu na podstawie ust. 1 zawierają co najmniej opis przedsiębiorstw, których dotyczy koncentracja, dane na temat ich rocznych obrotów w Unii i na świecie, ich obszarów działalności, w tym działalności bezpośrednio związanej z koncentracją, i wartości transakcyjnej umowy lub jej oszacowania, wraz ze skróconym opisem koncentracji, w tym jej charakteru i uzasadnienia, oraz wykazem państw członkowskich, których dotyczy dana koncentracja.

Informacje przekazane przez strażnika dostępu zawierają również, w odniesieniu do wszelkich odpowiednich podstawowych usług platformowych, dane na temat ich rocznych obrotów w Unii oraz, odpowiednio, liczby korzystających z tych usług użytkowników biznesowych aktywnych rocznie i liczby użytkowników końcowych aktywnych miesięcznie.

3. Jeżeli po przeprowadzeniu koncentracji, o której mowa w ust. 1 niniejszego artykułu, dodatkowe podstawowe usługi platformowe indywidualnie osiągną progi ustanowione w art. 3 ust. 2 lit. b), dany strażnik dostępu informuje o tym Komisję w terminie 2 miesięcy od dnia przeprowadzenia koncentracji i przekazuje Komisji informacje, o których mowa w art. 3 ust. 2.

4. Komisja informuje właściwe organy państw członkowskich o informacjach otrzymanych na podstawie ust. 1 i publikuje co roku wykaz przejęć, o których została poinformowana przez strażników dostępu na podstawie tego ustępu.

Komisja uwzględni uzasadniony interes przedsiębiorstw w odniesieniu do ochrony ich tajemnic handlowych.

5. Właściwe organy państw członkowskich mogą wykorzystać informacje otrzymane na podstawie ust. 1 niniejszego artykułu, aby zwrócić się do Komisji o zbadanie koncentracji na podstawie art. 22 rozporządzenia (WE) nr 139/2004.

#### Artykuł 15

### Obowiązek przeprowadzenia audytu

1. W terminie 6 miesięcy od dnia wskazania na podstawie art. 3 strażnik dostępu przedkłada Komisji poddany niezależnemu audytowi opis technik profilowania konsumentów, z których korzysta w odniesieniu do lub w ramach świadczonych przez siebie podstawowych usług platformowych wymienionych w decyzji o wskazaniu na podstawie z art. 3 ust. 9. Komisja przekazuje ten poddany audytowi opis Europejskiej Radzie Ochrony Danych.

2. Komisja może przyjąć akt wykonawczy, o którym mowa w art. 46 ust. 1 lit. g), w celu opracowania metodyki i procedury audytu.

3. Strażnik dostępu udostępnia publicznie podsumowanie opisu poddanego audytowi, o którym mowa w ust. 1. Udostępniając publicznie to podsumowanie strażnik dostępu jest uprawniony do uwzględnienia konieczności zachowania swoich tajemnic handlowych. Strażnik dostępu co najmniej raz w roku aktualizuje ten opis i jego podsumowanie.

## ROZDZIAŁ IV

### BADANIE RYNKU

#### Artykuł 16

### Rozpoczęcie badania rynku

1. Jeżeli Komisja zamierza przeprowadzić badanie rynku z myślą o możliwym przyjęciu decyzji na podstawie art. 17, 18 i 19, przyjmuje decyzję o rozpoczęciu badania rynku.

2. Niezależnie od ust. 1 Komisja może skorzystać ze swoich uprawnień w zakresie prowadzenia badań na podstawie niniejszego rozporządzenia przed rozpoczęciem badania rynku na podstawie tego ustępu.

3. W decyzji, o której mowa w ust. 1, należy określić:
  - a) datę rozpoczęcia badania rynku;
  - b) opis kwestii, której dotyczy badanie rynku;
  - c) cel badania rynku.
4. Komisja może ponownie rozpocząć badanie rynku, które zostało już zakończone, jeżeli:
  - a) nastąpiła istotna zmiana stanu faktycznego, na podstawie którego przyjęta została decyzja na podstawie art. 17, 18 lub 19; lub
  - b) decyzja przyjęta na podstawie art. 17, 18 lub 19 została podjęta na podstawie niekompletnych, nieprawdziwych lub wprowadzających w błąd informacji.
5. Komisja może zwrócić się do jednego lub większej liczby właściwych organów krajowych o udzielenie jej pomocy przy badaniu rynku.

#### Artykuł 17

### **Badanie rynku przeprowadzane w celu wskazania strażników dostępu**

1. Komisja może przeprowadzić badanie rynku w celu ustalenia, czy przedsiębiorstwo świadczące podstawowe usługi platformowe powinno zostać wskazane jako strażnik dostępu na podstawie art. 3 ust. 8, lub w celu zidentyfikowania podstawowych usług platformowych, które należy wymienić w decyzji o wskazaniu zgodnie z art. 3 ust. 9. Komisja dąży do zakończenia badania rynku w terminie 12 miesięcy od daty, o której mowa w art. 16 ust. 3 lit. a). W celu zakończenia badania rynku Komisja przyjmuje akt wykonawczy określający jej decyzję. Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.
2. W toku badania rynku przeprowadzanego na podstawie ust. 1 niniejszego artykułu Komisja dąży do przekazania swoich wstępnych ustaleń odpowiedniemu przedsiębiorstwu świadczącemu podstawowe usługi platformowe w terminie 6 miesięcy od daty, o której mowa w art. 16 ust. 3 lit. a). We wstępnych ustaleniach Komisja wyjaśnia, czy w jej wstępnej opinii należy wskazać przedsiębiorstwo jako strażnika dostępu na podstawie art. 3 ust. 8 i czy odpowiednie podstawowe usługi platformowe należy wymienić w wykazie na podstawie art. 3 ust. 9.
3. Jeżeli przedsiębiorstwo świadczące podstawowe usługi platformowe osiągnęło progi ustanowione w art. 3 ust. 2, ale przedstawiło zgodnie z art. 3 ust. 5 dostatecznie uzasadnione argumenty podważające w wyraźny sposób domniemanie określone w art. 3 ust. 2, Komisja dąży do zakończenia badania rynku w terminie 5 miesięcy od daty, o której mowa w art. 16 ust. 3 lit. a).

W takim przypadku Komisja dąży do przekazania zainteresowanemu przedsiębiorstwu wstępnych ustaleń zgodnie z ust. 2 niniejszego artykułu w terminie 3 miesięcy od daty, o której mowa w art. 16 ust. 3 lit. a).

4. Jeżeli Komisja, działając na podstawie art. 3 ust. 8, wskazuje jako strażnika dostępu przedsiębiorstwo świadczące podstawowe usługi platformowe, które nie ma jeszcze ugruntowanej i trwałej pozycji w zakresie prowadzonej działalności, ale prawdopodobnie zajmie taką pozycję w niedalekiej przyszłości, może ona stwierdzić, że w przypadku tego strażnika dostępu znajduje zastosowanie wyłącznie jeden lub więcej obowiązków ustanowionych w art. 5 ust. 3 - 6 oraz w art. 6 ust. 4, 7, 9, 10 i 13, zgodnie z tym, co określono w decyzji o wskazaniu. Komisja może stwierdzić, że znajdują zastosowanie tylko takie z tych obowiązków, które są stosowne i konieczne do zapobieżenia osiągnięciu w nieuczciwy sposób przez danego strażnika dostępu ugruntowanej i trwałej pozycji w zakresie prowadzonej przez niego działalności. Komisja dokonuje przeglądu takiego wskazania zgodnie z procedurą ustanowioną w art. 4.

## Artykuł 18

**Badanie rynku dotyczące systematycznego niewypełniania obowiązków**

1. Komisja może przeprowadzić badanie rynku w celu ustalenia, czy dany strażnik dostępu nie dopuszcza się systematycznego niewypełniania obowiązków. Komisja kończy to badanie rynku w terminie 12 miesięcy od daty, o której mowa w art. 16 ust. 3 lit. a). Jeżeli w wyniku badania rynku okaże się, że strażnik dostępu systematycznie nie wypełnia jednego lub więcej obowiązków ustanowionych w art. 5, 6 lub 7 i utrzymał, umocnił lub rozszerzył swoją pozycję strażnika dostępu, biorąc pod uwagę wymogi określone w art. 3 ust. 1, Komisja może przyjąć akt wykonawczy, w którym nakłada na takiego strażnika dostępu behawioralne lub strukturalne środki zaradcze, które są proporcjonalne i konieczne do zapewnienia skutecznego przestrzegania przepisów niniejszego rozporządzenia. Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.

2. Środek zaradczy nałożony zgodnie z ust. 1 niniejszego artykułu może obejmować – w zakresie, w jakim taki środek zaradczy jest proporcjonalny i konieczny do utrzymania lub przywrócenia uczciwości i kontestowalności, na które wpływa systematyczne niewypełnianie obowiązków – obowiązujący przez ograniczony okres zakaz zawierania przez strażnika dostępu umów dotyczących koncentracji w rozumieniu art. 3 rozporządzenia (WE) nr 139/2004 w odniesieniu do podstawowych usług platformowych lub innych usług świadczonych w sektorze cyfrowym lub umożliwiających zbieranie danych, na które wpływa systematyczne niewypełnianie obowiązków.

3. Przyjmuje się, że strażnik dostępu dopuszcza się systematycznego niewypełniania obowiązków ustanowionych w art. 5, 6 i 7, jeżeli Komisja wydała przeciwko takiemu strażnikowi dostępu co najmniej trzy decyzje w sprawie niewypełniania obowiązków na podstawie art. 29 w odniesieniu do dowolnej spośród świadczonych przez niego podstawowych usług platformowych w okresie 8 lat poprzedzających przyjęcie decyzji o rozpoczęciu badania rynku z myślą o możliwym przyjęciu decyzji na podstawie niniejszego artykułu.

4. Komisja przekazuje swoje wstępne ustalenia zainteresowanemu strażnikowi dostępu w terminie 6 miesięcy od daty, o której mowa w art. 16 ust. 3 lit. a). W swoich wstępnych ustaleniach Komisja wyjaśnia, czy wstępnie uznaje warunki określone w ust. 1 niniejszego artykułu za spełnione, oraz wskazuje, które środki zaradcze wstępnie uznaje za konieczne i proporcjonalne.

5. Aby umożliwić zainteresowanym osobom trzecim skuteczne zgłaszanie uwag, Komisja równocześnie z przekazaniem swoich wstępnych ustaleń strażnikowi dostępu na podstawie ust. 4 lub jak najszybciej po przekazaniu tych ustaleń publikuje jawne streszczenie zawierające opis danej sprawy i środków zaradczych, których nałożenie rozważa. Komisja określa rozsądny termin na zgłaszanie takich uwag.

6. W przypadku gdy Komisja zamierza przyjąć decyzję na podstawie ust. 1 niniejszego artykułu poprzez uczynienie wiążącymi zobowiązań zaproponowanych przez strażnika dostępu zgodnie z art. 25, publikuje jawne streszczenie zawierające opis danej sprawy oraz najważniejszych elementów tych zobowiązań. Zainteresowane osoby trzecie mogą zgłaszać uwagi w rozsądnym terminie określonym przez Komisję.

7. W toku badania rynku Komisja może przedłużyć okres prowadzenia tego badania, jeżeli takie przedłużenie jest uzasadnione ze względów obiektywnych i jeżeli jest proporcjonalne. Takie przedłużenie może również dotyczyć terminu na przekazanie przez Komisję jej wstępnych ustaleń lub terminu na przyjęcie przez nią ostatecznej decyzji. Łączny okres przedłużenia lub przedłużeń dokonanych na podstawie niniejszego ustępu nie może przekraczać 6 miesięcy.

8. Aby zapewnić skuteczne wypełnianie przez strażnika dostępu obowiązków ustanowionych w art. 5, 6 i 7, Komisja regularnie dokonuje przeglądu środków zaradczych, które nakłada zgodnie z ust. 1 i 2 niniejszego artykułu. Komisja jest uprawniona do zmiany tych środków zaradczych, jeżeli w wyniku nowego badania rynku stwierdzi, że nie są one skuteczne.

*Artykuł 19***Badanie rynku dotyczące nowych usług i nowych praktyk**

1. Komisja może przeprowadzić badanie rynku, aby ustalić, czy do wykazu podstawowych usług platformowych określonych w art. 2 pkt 2 należy dodać usługę lub większą liczbę usług świadczonych w sektorze cyfrowym, lub aby wykręcić praktyki, które ograniczają kontestowalność podstawowych usług platformowych lub są nieuczciwe, a którym nie zaradzono w skuteczny sposób w niniejszym rozporządzeniu. W swojej ocenie Komisja uwzględnia wszelkie istotne ustalenia z przeprowadzonych na podstawie art. 101 i 102 TFUE postępowań dotyczących rynków cyfrowych, a także inne istotne zmiany.
2. Przeprowadzając badanie rynku na podstawie ust. 1, Komisja może konsultować się z osobami trzecimi, w tym z użytkownikami biznesowymi i użytkownikami końcowymi badanych usług w sektorze cyfrowym oraz z użytkownikami biznesowymi i użytkownikami końcowymi, których dotyczą badane praktyki.
3. Komisja publikuje swoje ustalenia w formie sprawozdania w terminie 18 miesięcy od daty, o której mowa w art. 16 ust. 3 lit. a).

Sprawozdanie jest przedkładane Parlamentowi Europejskiemu i Radzie oraz towarzyszy mu w stosownych przypadkach:

- a) wniosek ustawodawczy w sprawie zmiany niniejszego rozporządzenia w celu zamieszczenia dodatkowych usług świadczonych w sektorze cyfrowym w wykazie podstawowych usług platformowych określonym w art. 2 pkt 2 lub zamieszczenia nowych obowiązków w rozdziale III; lub
- b) projekt aktu delegowanego uzupełniającego niniejsze rozporządzenie w odniesieniu do obowiązków ustanowionych w art. 5 i 6 lub projekt aktu delegowanego zmieniającego lub uzupełniającego niniejsze rozporządzenie w odniesieniu do obowiązków ustanowionych w art. 7, jak przewidziano w art. 12.

W stosownych przypadkach wniosek ustawodawczy w sprawie zmiany niniejszego rozporządzenia na podstawie lit. a) akapitu drugiego może również zawierać propozycję usunięcia istniejących usług z wykazu podstawowych usług platformowych określonego w art. 2 pkt 2 lub usunięcia istniejących obowiązków z art. 5, 6 lub 7.

## ROZDZIAŁ V

**UPRAWNIENIA W ZAKRESIE PROWADZENIA BADAŃ ORAZ EGZEKOWANIA I MONITOROWANIA***Artykuł 20***Wszczęcie postępowania**

1. Jeżeli Komisja zamierza wszcząć postępowanie z myślą o możliwym przyjęciu decyzji na podstawie art. 8, 29 i 30, przyjmuje decyzję o wszczęciu postępowania.
2. Niezależnie od ust. 1 Komisja może skorzystać ze swoich uprawnień w zakresie prowadzenia badań na podstawie niniejszego rozporządzenia przed rozpoczęciem postępowania na podstawie tego ustępu.

*Artykuł 21***Wnioski o udzielenie informacji**

1. W celu wykonywania zadań wynikających z niniejszego rozporządzenia Komisja może zażądać – w drodze zwykłego wniosku lub decyzji – od przedsiębiorstw lub związków przedsiębiorstw udzielenia wszelkich koniecznych informacji. Komisja może również – w drodze zwykłego wniosku lub decyzji – zażądać udzielenia jej dostępu do danych i algorytmów przedsiębiorstw oraz informacji o testach, a także zażądać udzielenia jej wyjaśnień w tym zakresie.

2. Jeżeli Komisja żąda od przedsiębiorstw lub związków przedsiębiorstw udzielenia informacji w drodze zwykłego wniosku, podaje podstawę prawną i cel takiego żądania, określa zakres żądanych informacji, wyznacza termin, w którym należy je dostarczyć, jak również poucza o grzywnach przewidzianych w art. 30 mających zastosowanie w przypadku udzielenia niekompletnych, nieprawdziwych lub wprowadzających w błąd informacji lub wyjaśnień.
3. Jeżeli Komisja żąda od przedsiębiorstw lub związków przedsiębiorstw udzielenia informacji w drodze decyzji, podaje podstawę prawną i cel takiego żądania, określa zakres żądanych informacji i wyznacza termin, w którym należy je dostarczyć. Jeżeli Komisja żąda od przedsiębiorstw zapewnienia dostępu do danych i algorytmów oraz informacji o testach, podaje cel takiego żądania oraz wyznacza termin, w którym należy zapewnić ten dostęp i te informacje. Komisja poucza także o grzywnach przewidzianych w art. 30 oraz poucza o okresowych karach pieniężnych przewidzianych w art. 31 lub nakłada takie kary pieniężne. Poucza ona również o prawie do kontroli tej decyzji przez Trybunał Sprawiedliwości.
4. Przedsiębiorstwa lub związki przedsiębiorstw lub ich przedstawiciele przekazują żądane informacje w imieniu odpowiedniego przedsiębiorstwa lub związku przedsiębiorstw. Prawnicy należycie upoważnieni do działania mogą przekazywać informacje w imieniu swoich klientów. Klienci pozostają w pełni odpowiedzialni, jeżeli przekazane informacje są niekompletne, nieprawdziwe lub wprowadzające w błąd.
5. Na wniosek Komisji właściwe organy państw członkowskich udzielają Komisji wszelkich informacji, które znajdują się w ich posiadaniu, koniecznych do wykonywania zadań powierzonych jej niniejszym rozporządzeniem.

#### Artykuł 22

### Uprawnienie do odbierania wyjaśnień i przyjmowania oświadczeń

1. W celu wykonywania zadań wynikających z niniejszego rozporządzenia Komisja może odbierać wyjaśnienia od wszelkich osób fizycznych lub prawnych, które wyrażą zgodę na złożenie wyjaśnień, w celu zebrania informacji odnoszących się do przedmiotu badania. Komisja jest uprawniona do rejestrowania takich wyjaśnień za pomocą wszelkich środków technicznych.
2. Gdy odbieranie wyjaśnień zgodnie z ust. 1 niniejszego artykułu prowadzone jest w pomieszczeniach przedsiębiorstwa, Komisja informuje o tym odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego, na terytorium którego odbywa się odbieranie wyjaśnień. Na wniosek tego właściwego organu, jego urzędnicy mogą pomagać urzędnikom i innym towarzyszącym osobom upoważnionym przez Komisję do odbierania wyjaśnień.

#### Artykuł 23

### Uprawnienia do przeprowadzania kontroli

1. W celu wykonywania zadań wynikających z niniejszego rozporządzenia Komisja może przeprowadzać wszelkie konieczne kontrole przedsiębiorstw lub związków przedsiębiorstw.
2. Urzędnicy i inne towarzyszące osoby upoważnione przez Komisję do przeprowadzania kontroli mają prawo:
  - a) wstępu do wszelkich pomieszczeń, na teren i do środków transportu przedsiębiorstw i związków przedsiębiorstw;
  - b) sprawdzać księgi i inne rejestry związane z działalnością gospodarczą, niezależnie od nośnika, na jakim są przechowywane;
  - c) pobierać lub uzyskiwać, w dowolnej formie, kopie lub wyciągi z takich ksiąg lub rejestrów;
  - d) wymagać od przedsiębiorstwa lub związku przedsiębiorstw udzielenia dostępu do ich organizacji, działalności, systemu informatycznego, algorytmów, przetwarzania danych i praktyk biznesowych oraz przedstawienia wyjaśnień na temat tych elementów, a następnie rejestrować lub udokumentować wyjaśnienia udzielone za pomocą wszelkich środków technicznych;
  - e) pieczętować wszelkie pomieszczenia przedsiębiorstwa i księgi lub rejestry na czas i w zakresie koniecznym do przeprowadzenia kontroli;

f) zadawać pytania przedstawicielom lub członkom personelu przedsiębiorstwa lub związku przedsiębiorstw w celu uzyskania wyjaśnień co do faktów lub dokumentów dotyczących przedmiotu i celu kontroli oraz rejestrować za pomocą wszelkich środków technicznych odpowiedzi.

3. Aby przeprowadzać kontrole, Komisja może zwrócić się o pomoc audytorów lub ekspertów powołanych przez Komisję na podstawie art. 26 ust. 2, a także o pomoc odpowiedzialnego za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwego organu krajowego państwa członkowskiego, na terytorium którego ma być przeprowadzona kontrola.

4. Podczas kontroli Komisja, audytorzy lub eksperci przez nią powołani oraz odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego, na terytorium którego ma być przeprowadzona kontrola, mogą zażądać od przedsiębiorstwa lub związku przedsiębiorstw udzielenia dostępu do ich organizacji, działalności, systemu informatycznego, algorytmów, przetwarzania danych i praktyk biznesowych oraz przedstawienia wyjaśnień na temat tych elementów. Komisja i audytorzy lub eksperci przez nią powołani oraz odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego, na terytorium którego ma być przeprowadzona kontrola, mogą zadawać pytania każdemu przedstawicielowi lub członkowi personelu.

5. Urzędnicy i inne towarzyszące osoby upoważnione przez Komisję do przeprowadzenia kontroli wykonują swoje uprawnienia po okazaniu pisemnego upoważnienia zawierającego określenie przedmiotu i celu kontroli oraz pouczenie o grzywnach przewidzianych w art. 30 mających zastosowanie w przypadku gdy okazane księgi i rejestry związane z działalnością gospodarczą są niekompletne lub gdy odpowiedzi na pytania zadane zgodnie z ust. 2 i 4 niniejszego artykułu są nieprawdziwe lub wprowadzające w błąd. Z odpowiednim wyprzedzeniem przed rozpoczęciem kontroli Komisja powiadomi o niej odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego, na terytorium którego ma być przeprowadzona kontrola.

6. Przedsiębiorstwa lub związki przedsiębiorstw są zobowiązane poddać się kontroli zarządzanej decyzją Komisji. Decyzja ta określa przedmiot i cel kontroli, termin jej rozpoczęcia i pouczenie o grzywnach i okresowych karach pieniężnych przewidzianych odpowiednio w art. 30 i 31 oraz o prawie do kontroli tej decyzji przez Trybunał Sprawiedliwości.

7. Na wniosek odpowiedzialnego za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwego organu krajowego państwa członkowskiego, na terytorium którego ma być przeprowadzona kontrola, lub na wniosek Komisji urzędnicy właściwego organu oraz upoważnione bądź powołane przez niego osoby aktywnie pomagają urzędnikom i innym osobom towarzyszącym upoważnionym przez Komisję. W tym celu przysługują im uprawnienia określone w ust. 2 i 4 niniejszego artykułu.

8. W przypadku gdy urzędnicy i inne osoby towarzyszące upoważnione przez Komisję stwierdzą, że przedsiębiorstwo lub związek przedsiębiorstw sprzeciwia się kontroli zarządzanej zgodnie z niniejszym artykułem, odpowiednie państwo członkowskie udziela im niezbędnej pomocy, zwracając się w razie potrzeby o pomoc policji lub równorzędnego organu egzekwowania prawa, w celu umożliwienia im przeprowadzenia kontroli.

9. Jeżeli zgodnie z przepisami krajowymi pomoc, o której mowa w ust. 8 niniejszego artykułu, wymaga zezwolenia organu sądowego, Komisja lub odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego lub urzędnicy upoważnieni przez te organy występują o wydanie takiego zezwolenia. O wydanie takiego zezwolenia można również wystąpić jako o środek zapobiegawczy.

10. W przypadku gdy wystąpiono o zezwolenie, o którym mowa w ust. 9 niniejszego artykułu, krajowy organ sądowy sprawdza, czy decyzja Komisji jest autentyczna, przewidziane środki przymusu nie są arbitralne ani nadmiernie uciążliwe w stosunku do przedmiotu kontroli. Badając proporcjonalność środków przymusu, krajowe organy sądowe mogą wystąpić do Komisji, bezpośrednio lub za pośrednictwem odpowiedzialnego za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwego organu krajowego państwa członkowskiego, o szczegółowe wyjaśnienia dotyczące w szczególności podstaw, na jakich Komisja powzięła podejrzenie o naruszeniu niniejszego rozporządzenia, jak również o wyjaśnienia dotyczące wagi podejrzanego naruszenia oraz charakteru uczestnictwa w nim danego przedsiębiorstwa. Krajowy organ sądowy nie może jednak kwestionować konieczności przeprowadzenia kontroli ani żądać udzielenia informacji zawartych w aktach Komisji. Legalność decyzji Komisji może być rozpatrywana jedynie przez Trybunał Sprawiedliwości.



## Artykuł 24

**Środki tymczasowe**

W przypadkach naglących ze względu na ryzyko zaistnienia poważnej i nieodwracalnej szkody dla użytkowników biznesowych lub użytkowników końcowych strażnika dostępu, Komisja może przyjąć akt wykonawczy zarządzający środkami tymczasowymi przeciwko strażnikowi dostępu na podstawie stwierdzenia *prima facie*, że doszło do naruszenia art. 5, 6 lub 7. Akt wykonawczy przyjmuje się wyłącznie w ramach postępowania wszczętego z myślą o możliwym przyjęciu decyzji stwierdzającej niewypełnianie obowiązków na podstawie art. 29 ust. 1. Obowiązuje on wyłącznie przez czas oznaczony, który może zostać przedłużony, jeżeli to konieczne i stosowne. Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.

## Artykuł 25

**Zobowiązania**

1. Jeżeli w toku postępowania, o którym mowa w art. 18, strażnik dostępu zaproponuje podjęcie zobowiązań odnoszących się do odpowiednich podstawowych usług platformowych i mających na celu wypełnienie obowiązków ustanowionych w art. 5, 6 i 7, Komisja może przyjąć akt wykonawczy czyniący te zobowiązania wiążącymi dla danego strażnika dostępu oraz oświadczyć, że nie ma dalszych podstaw do prowadzenia postępowania. Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.
2. Komisja może, na wniosek lub z własnej inicjatywy, wznowić stosowne postępowanie w drodze decyzji, jeżeli:
  - a) nastąpiła istotna zmiana stanu faktycznego, na podstawie którego podjęta została decyzja;
  - b) dany strażnik dostępu działa w sposób sprzeczny ze swoimi zobowiązaniami;
  - c) decyzja została podjęta na podstawie niekompletnych, nieprawdziwych lub wprowadzających w błąd informacji dostarczonych przez strony;
  - d) zobowiązania nie są skuteczne.
3. Jeżeli Komisja uzna, że zobowiązania zaproponowane przez danego strażnika dostępu nie zapewniają skutecznego wypełniania obowiązków ustanowionych w art. 5, 6 i 7, uzasadnia w decyzji kończącej dane postępowanie, dlaczego nie uczyniła tych zobowiązań wiążącymi.

## Artykuł 26

**Monitorowanie obowiązków i środków**

1. Komisja podejmuje działania konieczne w celu monitorowania skutecznego wdrażania i wypełniania obowiązków ustanowionych w art. 5, 6 i 7 oraz skutecznego wdrażania i przestrzegania decyzji przyjętych na podstawie art. 8, 18, 24, 25 i 29. Działania te mogą obejmować w szczególności nałożenie na strażnika dostępu obowiązku przechowywania wszystkich dokumentów uznanych za istotne dla oceny wdrażania i wypełniania tych obowiązków oraz wdrażania i przestrzegania tych decyzji.
2. Działania, o których mowa w ust. 1, mogą obejmować powołanie niezależnych zewnętrznych ekspertów i audytorów, a także powołanie urzędników z właściwych organów krajowych państw członkowskich celem udzielenia Komisji pomocy w zakresie monitorowania wypełniania obowiązków i stosowania się do środków oraz zapewnienia Komisji konkretnej wiedzy, w tym wiedzy specjalistycznej.

## Artykuł 27

**Informacje od osób trzecich**

1. Każda osoba trzecia, w tym użytkownicy biznesowi, konkurenci lub użytkownicy końcowi podstawowych usług platformowych wymienionych w decyzji o wskazaniu zgodnie z art. 3 ust. 9, jak również ich przedstawiciele, mogą informować odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego lub bezpośrednio Komisję o wszelkich praktykach lub zachowaniach strażników dostępu, które są objęte zakresem stosowania niniejszego rozporządzenia.

2. Odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego oraz Komisja mają pełną swobodę decydowania o odpowiednich środkach oraz są zobowiązane podejmować działań w reakcji na uzyskane informacje.

3. Jeżeli odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego stwierdzi, w oparciu o informacje uzyskane zgodnie z ust. 1 niniejszego artykułu, że może zachodzić przypadek nieprzestrzegania niniejszego rozporządzenia, przekazuje tę informację Komisji.

#### Artykuł 28

### **Komórka nadzoru przestrzegania niniejszego rozporządzenia**

1. Strażnicy dostępu ustanawiają komórkę nadzoru przestrzegania niniejszego rozporządzenia, która jest niezależna od komórek operacyjnych strażnika dostępu i składa się z co najmniej jednego pracownika ds. nadzoru przestrzegania niniejszego rozporządzenia, w tym kierownika komórki nadzoru przestrzegania niniejszego rozporządzenia.

2. Strażnik dostępu zapewnia, by komórka nadzoru przestrzegania niniejszego rozporządzenia, o której mowa w ust. 1, dysponowała wystarczającymi uprawnieniami i zasobami, posiadała odpowiedni status, a także miała dostęp do organu zarządzającego strażnika dostępu w celu monitorowania zachowania przez strażnika dostępu zgodności z niniejszym rozporządzeniem.

3. Organ zarządzający strażnika dostępu zapewnia, by pracownicy ds. nadzoru przestrzegania niniejszego rozporządzenia powołani zgodnie z ust. 1 mieli kwalifikacje zawodowe, wiedzę, doświadczenie i umiejętności niezbędne do wykonywania zadań, o których mowa w ust. 5.

Organ zarządzający strażnika dostępu zapewnia także, by taki kierownik komórki nadzoru przestrzegania niniejszego rozporządzenia był niezależnym członkiem kierownictwa wyższego szczebla, któremu wyraźnie powierzono odpowiedzialność za tę komórkę.

4. Kierownik komórki nadzoru przestrzegania niniejszego rozporządzenia podlega bezpośrednio organowi zarządzającemu strażnika dostępu i może zgłaszać obawy i ostrzegać ten organ w przypadku wystąpienia ryzyka braku zgodności z niniejszym rozporządzeniem, bez uszczerbku dla obowiązków organu zarządzającego w ramach jego funkcji nadzorczych i zarządczych.

Kierownik komórki nadzoru przestrzegania niniejszego rozporządzenia nie może zostać odwołany bez uprzedniej zgody organu zarządzającego strażnika dostępu.

5. Pracownicy ds. nadzoru przestrzegania niniejszego rozporządzenia powołani przez strażnika dostępu zgodnie z ust. 1 realizują następujące zadania:

- a) organizowanie, monitorowanie i nadzorowanie środków i działań strażników dostępu mających na celu zapewnienie zgodności z niniejszym rozporządzeniem;
- b) przekazywanie informacji i doradzanie kierownictwu i pracownikom strażnika dostępu w sprawach zapewniania zgodności z niniejszym rozporządzeniem;
- c) w stosownych przypadkach – monitorowanie wywiązywania się z zobowiązań, które uczyniono wiążącymi zgodnie z art. 25, bez uszczerbku dla możliwości powoływania przez Komisję niezależnych ekspertów zewnętrznych zgodnie z art. 26 ust. 2;
- d) współpraca z Komisją do celów niniejszego rozporządzenia.

6. Strażnicy dostępu przekazują Komisji imię i nazwisko oraz dane kontaktowe kierownika komórki nadzoru przestrzegania niniejszego rozporządzenia.

7. Organ zarządzający strażnika dostępu określa i nadzoruje rozwiązania w zakresie zarządzania, które zapewniają niezależność komórki nadzoru przestrzegania niniejszego rozporządzenia, w tym podział obowiązków w organizacji strażnika dostępu i zapobieganie konfliktom interesów, oraz odpowiada za wdrażanie tych rozwiązań.

8. Organ zarządzający zatwierdza strategię i politykę zapewniania i monitorowania zgodności z niniejszym rozporządzeniem oraz zarządzania nią, a także co najmniej raz w roku dokonuje ich przeglądu.

9. Organ zarządzający poświęca odpowiednio dużo czasu monitorowaniu zgodności z niniejszym rozporządzeniem i zarządzaniu nią. Aktywnie uczestniczy on w decyzjach dotyczących zarządzania w odniesieniu do niniejszego rozporządzenia i jego wykonywania oraz zapewnia, by na te cele przydzielane były odpowiednie zasoby.

#### Artykuł 29

### Niewypełnianie obowiązków

1. Komisja przyjmuje akt wykonawczy zawierający jej stwierdzenie dotyczące niewypełniania obowiązków (zwany dalej „decyzją stwierdzającą niewypełnianie obowiązków”), jeżeli uzna, że strażnik dostępu:

- a) nie wypełnia któregokolwiek z obowiązków ustanowionych w art. 5, 6 lub 7;
- b) nie zastosował się do środków doprecyzowanych przez Komisję w decyzji przyjętej na podstawie art. 8 ust. 2;
- c) nie zastosował się do środków zaradczych nałożonych na podstawie art. 18 ust. 1;
- d) nie zastosował się do środków tymczasowych zarządzonych na podstawie art. 24; lub
- e) nie wykonał zobowiązań, które uczyniono prawnie wiążącymi na podstawie art. 25.

Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.

2. Komisja dąży do przyjęcia decyzji stwierdzającej niewypełnianie obowiązków w terminie 12 miesięcy od dnia wszczęcia postępowania na podstawie art. 20.

3. Przed przyjęciem decyzji stwierdzającej niewypełnianie obowiązków Komisja przedstawia swoje wstępne ustalenia danemu strażnikowi dostępu. W tych wstępnych ustaleniach Komisja wyjaśnia środki, których wprowadzenie rozważa lub które jej zdaniem dany strażnik dostępu powinien wprowadzić w celu skutecznego zastosowania się do wstępnych ustaleń.

4. Przed przyjęciem decyzji stwierdzającej niewypełnianie obowiązków Komisja może konsultować się z osobami trzecimi.

5. W decyzji stwierdzającej niewypełnianie obowiązków Komisja nakazuje strażnikowi dostępu zaprzestać i zaniechać niewypełniania obowiązków w stosownym terminie oraz przedstawić wyjaśnienia dotyczące sposobu, w jaki zamierza on zastosować się do tej decyzji.

6. Strażnik dostępu przedstawia Komisji opis środków, które wprowadził w celu zapewnienia wykonania decyzji stwierdzającej niewypełnianie obowiązków.

7. W przypadku gdy Komisja postanowi nie przyjmować decyzji stwierdzającej niewypełnianie obowiązków, kończy postępowanie w drodze decyzji.

#### Artykuł 30

### Grzywny

1. Komisja może w drodze decyzji stwierdzającej niewypełnianie obowiązków nałożyć na strażnika dostępu grzywny, których wysokość nie może przekraczać 10 % jego łącznego światowego obrotu uzyskanego w poprzednim roku obrotowym, jeżeli Komisja stwierdzi, że strażnik dostępu umyślnie lub w wyniku zaniedbania:

- a) nie wypełnił któregokolwiek z obowiązków ustanowionych w art. 5, 6 i 7;
- b) nie zastosował się do środków doprecyzowanych przez Komisję w decyzji przyjętej na podstawie art. 8 ust. 2;
- c) nie zastosował się do środków zaradczych nałożonych na podstawie art. 18 ust. 1;
- d) nie zastosował się do środków tymczasowych zarządzonych na podstawie art. 24; lub
- e) nie wykonał zobowiązań, które uczyniono prawnie wiążącymi na podstawie art. 25.

2. Bez uszczerbku dla ust. 1 niniejszego artykułu Komisja może w decyzji stwierdzającej niewypełnianie obowiązków nałożyć na strażnika dostępu grzywny w wysokości do 20 % jego łącznego światowego obrotu uzyskanego w poprzednim roku obrotowym, jeżeli stwierdzi, że strażnik dostępu w taki sam lub podobny sposób naruszył obowiązek ustanowiony w art. 5, 6 lub 7 w odniesieniu do tej samej podstawowej usługi platformowej, co ustalono w decyzji stwierdzającej niewypełnianie obowiązków przyjętej w ciągu 8 poprzednich lat.

3. Komisja może przyjąć decyzję nakładającą na przedsiębiorstwa, w tym w stosownych przypadkach na strażników dostępu, oraz na związki przedsiębiorstw grzywny, których wysokość nie może przekraczać 1 % ich łącznego światowego obrotu uzyskanego w poprzednim roku obrotowym, jeżeli umyślnie lub w wyniku zaniedbania:

- a) nie przekazali w terminie informacji wymaganych do oceny ich wskazania jako strażników dostępu zgodnie z art. 3 lub przekazali informacje nieprawdziwe, niekompletne lub wprowadzające w błąd;
- b) nie wypełnili obowiązku powiadomienia Komisji zgodnie z art. 3 ust. 3;
- c) nie przekazali informacji wymaganych na podstawie art. 14 lub przekazali informacje nieprawdziwe, niekompletne lub wprowadzające w błąd;
- d) nie przekazali opisu wymaganego na podstawie art. 15 lub przekazali informacje nieprawdziwe, niekompletne lub wprowadzające w błąd;
- e) nie zapewnili dostępu do danych, algorytmów lub informacji o testach w odpowiedzi na żądanie skierowane zgodnie z art. 21 ust. 3;
- f) nie przekazali żądanych informacji w terminie wyznaczonym zgodnie z art. 21 ust. 3 lub przekazali nieprawdziwe, niekompletne lub wprowadzające w błąd informacje lub wyjaśnienia, których zażądano zgodnie z art. 21 lub których udzielono w toku składania wyjaśnień zgodnie z art. 22;
- g) nie sprostowali w terminie wyznaczonym przez Komisję nieprawdziwych, niekompletnych lub wprowadzających w błąd informacji udzielonych przez przedstawiciela lub członka personelu lub też nie udzielili lub odmówili udzielenia kompletnych informacji na temat faktów związanych z przedmiotem i celem kontroli zgodnie z art. 23;
- h) odmówili poddania się kontroli prowadzonej na podstawie art.23;
- i) nie wypełnili obowiązków nałożonych przez Komisję na podstawie art. 26;
- j) nie ustanowili komórki nadzoru przestrzegania niniejszego rozporządzenia zgodnie z art. 28; lub
- k) nie przestrzegali warunków dostępu do akt Komisji określonych w art. 34 ust. 4.

4. Ustalając kwotę grzywny, Komisja uwzględni ciężar, czas trwania i powtarzalność naruszenia oraz, w przypadku grzywien nakładanych na podstawie ust. 3, opóźnienie spowodowane w postępowaniu.

5. Jeżeli grzywna nałożona na związek przedsiębiorstw uwzględni światowy obrót uzyskany przez jego członków, a związek ten nie jest wypłacalny, jest on zobowiązany do wezwania swoich członków do wniesienia wkładów w celu pokrycia kwoty grzywny.

Jeżeli wkład taki nie zostanie wniesiony do związku przedsiębiorstw w terminie wyznaczonym przez Komisję, Komisja może żądać zapłaty grzywny bezpośrednio od dowolnego przedsiębiorstwa, którego przedstawiciele byli członkami organów decyzyjnych danego związku.

Po zażądaniu zapłaty zgodnie z akapitem drugim Komisja może zażądać zapłaty pozostałej kwoty przez dowolnego członka związku przedsiębiorstw, jeżeli jest to konieczne do zapewnienia pełnej zapłaty grzywny.

Komisja nie może jednak żądać zapłaty na podstawie akapitu drugiego lub trzeciego od przedsiębiorstw, które wykazały, że nie wykonały decyzji związku przedsiębiorstw powodującej naruszenie niniejszego rozporządzenia oraz że nie wiedziały o jej istnieniu albo aktywnie dystansowały się od niej, zanim Komisja wszczęła postępowanie na podstawie art. 20.

Odpowiedzialność finansowa każdego przedsiębiorstwa w zakresie zapłaty grzywny nie może przekraczać 20 % jego łącznego światowego obrotu uzyskanego w poprzednim roku obrotowym.

### Artykuł 31

#### Okresowe kary pieniężne

1. Komisja może przyjąć decyzję nakładającą na przedsiębiorstwa, w tym w stosownych przypadkach na strażników dostępu, oraz na związki przedsiębiorstw okresowe kary pieniężne, których wysokość nie może przekraczać 5 % średniego dziennego światowego obrotu uzyskanego w poprzednim roku obrotowym i które są naliczane od daty ustalonej w decyzji, aby nakłonić przedsiębiorstwa do:

- a) zastosowania się do środków doprecyzowanych przez Komisję w decyzji przyjętej na podstawie art. 8 ust. 2;
- b) wykonania decyzji przyjętej na podstawie art. 18 ust. 1;
- c) dostarczenia prawdziwych i kompletnych informacji w terminie wyznaczonym w żądaniu udzielenia informacji skierowanym w drodze decyzji przyjętej na podstawie art. 21;
- d) zapewnienia dostępu do baz, algorytmów i informacji o testach w odpowiedzi na żądanie skierowane zgodnie z art. 21 ust. 3 oraz dostarczenia wyjaśnień w ich sprawie zgodnie z decyzją przyjętą na podstawie art. 21;
- e) poddania się kontroli zarządzanej decyzją przyjętą na podstawie art. 23;
- f) wykonania decyzji zarządzającej środki tymczasowe, przyjętej na podstawie art. 24;
- g) wykonania zobowiązań, które uczyniono prawnie wiążącymi w drodze decyzji przyjętej na podstawie art. 25 ust. 1;
- h) wykonania decyzji przyjętej na podstawie art. 29 ust. 1.

2. W przypadku gdy przedsiębiorstwa lub związki przedsiębiorstw wypełniły obowiązek, w odniesieniu do którego nałożono okresową karę pieniężną w celu jego wyegzekwowania, Komisja może przyjąć akt wykonawczy ustalający ostateczną wysokość okresowej kary pieniężnej na poziomie niższym niż ten, który wynikałby z pierwotnej decyzji. Akt wykonawczy przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.

### Artykuł 32

#### Terminy przedawnienia dotyczące nakładania sankcji

1. Uprawnienia przyznane Komisji na podstawie art. 30 i 31 podlegają przedawnieniu wynoszącemu 5 lat.
2. Bieg terminu przedawnienia rozpoczyna się od dnia, w którym popełniono naruszenie. Jednak w przypadku ciągłych lub powtarzających się naruszeń bieg terminu przedawnienia rozpoczyna się od dnia zaprzestania naruszenia.
3. Wszelkie działania podjęte przez Komisję w celu przeprowadzenia badania rynku lub postępowania w odniesieniu do naruszenia przerywają bieg terminu przedawnienia dotyczącego nakładania grzywnien lub okresowych kar pieniężnych. Bieg terminu przedawnienia uznaje się za przerwany ze skutkiem od dnia, w którym co najmniej jedno przedsiębiorstwo lub związek przedsiębiorstw, które uczestniczyły w naruszeniu, zostaną powiadomione o podjętych działaniach. Bieg terminu przedawnienia przerywają w szczególności:

- a) żądanie udzielenia informacji wystosowane przez Komisję;
- b) pisemne upoważnienia do przeprowadzania kontroli udzielone przez Komisję jej urzędnikom;
- c) wszczęcie postępowania przez Komisję na podstawie art. 20.

4. Każde przerwanie terminu przedawnienia powoduje, że termin ten zaczyna biec od początku. Termin przedawnienia upływa jednak najpóźniej w dniu, w którym upływa okres odpowiadający podwójnemu terminowi przedawnienia, a Komisja nie nałożyła grzywny lub okresowej kary pieniężnej. Termin ten przedłuża się o okres, na który bieg terminu przedawnienia został zawieszony na podstawie ust. 5.

5. Bieg terminu przedawnienia dotyczącego nakładania grzywnien lub okresowych kar pieniężnych ulega zawieszeniu na okres, przez który decyzja Komisji jest przedmiotem postępowania toczącego się przed Trybunałem Sprawiedliwości.

### Artykuł 33

#### Terminy przedawnienia dotyczące wykonania sankcji

1. Uprawnienia Komisji do wykonania decyzji przyjętych na podstawie art. 30 i 31 podlegają przedawnieniu wynoszącemu 5 lat.
2. Termin przedawnienia biegnie od dnia, w którym decyzja stała się ostateczna.
3. Bieg terminu przedawnienia dotyczącego wykonania sankcji przerywa:
  - a) powiadomienie o decyzji o zmianie pierwotnej kwoty grzywny lub okresowej kary pieniężnej lub o odrzuceniu wniosku o taką zmianę; lub
  - b) każde działanie Komisji lub państwa członkowskiego działające na wniosek Komisji mające na celu wyegzekwowanie zapłaty grzywny lub okresowej kary pieniężnej.
4. Każde przerwanie terminu przedawnienia powoduje, że termin ten zaczyna biec od początku.
5. Bieg terminu przedawnienia dotyczącego wykonania sankcji ulega zawieszeniu:
  - a) do upływu terminu przyznanego na zapłatę; lub
  - b) na czas zawieszenia egzekucji płatności na podstawie postanowienia Trybunału Sprawiedliwości lub orzeczenia sądu krajowego.

### Artykuł 34

#### Prawo do bycia wysłuchanym i prawo dostępu do akt

1. Przed przyjęciem decyzji na podstawie art. 8, art. 9 ust. 1, art. 10 ust. 1, art. 17, 18, 24, 25, 29 i 30 oraz art. 31 ust. 2 Komisja zapewnia zainteresowanemu strażnikowi dostępu lub zainteresowanemu przedsiębiorstwu lub zainteresowanemu związkowi przedsiębiorstw możliwość bycia wysłuchanym w sprawie:
  - a) wstępnych ustaleń Komisji, w tym w każdej kwestii, w której Komisja zgłosiła zastrzeżenia; oraz
  - b) środków, które Komisja może zamierzać wprowadzić w świetle wstępnych ustaleń zgodnie z lit. a) niniejszego ustępu.
2. Zainteresowani strażnicy dostępu, zainteresowane przedsiębiorstwa i zainteresowane związki przedsiębiorstw mogą przedstawić Komisji swoje uwagi dotyczące jej wstępnych ustaleń w terminie wyznaczonym przez Komisję we wstępnych ustaleniach, przy czym termin ten nie może być krótszy niż 14 dni.

3. Podstawą decyzji przyjmowanych przez Komisję mogą być wyłącznie wstępne ustalenia, w tym w każdej kwestii, w której Komisja zgłosiła zastrzeżenia, co do których zainteresowani strażnicy dostępu, zainteresowane przedsiębiorstwa i zainteresowane związki przedsiębiorstw mogli przedstawić swoje uwagi.

4. W toku postępowania w pełni respektuje się prawo zainteresowanego strażnika dostępu, zainteresowanego przedsiębiorstwa lub zainteresowanego związku przedsiębiorstw do obrony. Zainteresowany strażnik dostępu, zainteresowane przedsiębiorstwo lub zainteresowany związek przedsiębiorstw mają prawo dostępu do akt Komisji na warunkach ujawnienia, z zastrzeżeniem uzasadnionego interesu przedsiębiorstw w zakresie ochrony ich tajemnic handlowych. W przypadku braku porozumienia między stronami Komisja może przyjmować decyzje określające te warunki ujawnienia. Prawo dostępu do akt Komisji nie obejmuje informacji poufnych i dokumentów wewnętrznych Komisji ani właściwych organów państw członkowskich. W szczególności prawo dostępu nie obejmuje korespondencji między Komisją a właściwymi organami państw członkowskich. Żaden przepis niniejszego ustępu nie uniemożliwia Komisji ujawnienia i wykorzystania informacji koniecznych do udowodnienia naruszenia.

### Artykuł 35

#### **Sprawozdawczość roczna**

1. Komisja przedkłada Parlamentowi Europejskiemu i Radzie roczne sprawozdanie z wykonania niniejszego rozporządzenia oraz z postępów w realizacji jego celów.
2. Sprawozdanie, o którym mowa w ust. 1, zawiera:
  - a) podsumowanie działań Komisji, w tym informacje o wszelkich podjętych środkach i przyjętych decyzjach oraz trwających badaniach rynku związanych z niniejszym rozporządzeniem;
  - b) ustalenia z monitorowania wypełniania przez strażników dostępu obowiązków wynikających z niniejszego rozporządzenia;
  - c) ocenę poddanego audytowi opisu, o którym mowa w art. 15;
  - d) podsumowanie współpracy między Komisją a organami krajowymi w odniesieniu do niniejszego rozporządzenia;
  - e) podsumowanie działań i zadań Grupy Wysokiego Szczebla Organów Regulacji Cyfrowej, w tym sposobów wdrażania jej zaleceń dotyczących wykonywania niniejszego rozporządzenia.
3. Komisja publikuje to sprawozdanie na swojej stronie internetowej.

### Artykuł 36

#### **Tajemnica zawodowa**

1. Informacje zebrane na podstawie niniejszego rozporządzenia wykorzystuje się do celów niniejszego rozporządzenia.
2. Informacje zebrane na podstawie art. 14 wykorzystuje się do celów niniejszego rozporządzenia, rozporządzenia (WE) nr 139/2004 i krajowych przepisów dotyczących łączenia przedsiębiorstw.
3. Informacje zebrane na podstawie art. 15 wykorzystuje się do celów niniejszego rozporządzenia i rozporządzenia (UE) 2016/679.
4. Bez uszczerbku dla wymiany i wykorzystywania informacji przekazywanych w celu wykorzystania ich na podstawie art. 38, 39, 41 i 43 Komisja, właściwe organy państw członkowskich, ich urzędnicy, funkcjonariusze i inne osoby pracujące pod nadzorem tych organów oraz osoby fizyczne lub prawne, w tym audytorzy i eksperci powołani na podstawie art. 26 ust. 2, nie ujawniają informacji uzyskanych lub wymienionych przez nich na podstawie niniejszego rozporządzenia oraz objętych obowiązkiem zachowania tajemnicy zawodowej.

*Artykuł 37***Współpraca z organami krajowymi**

1. Komisja i państwa członkowskie ściśle współpracują i koordynują swoje działania w zakresie egzekwowania w celu zapewnienia spójnego, skutecznego i komplementarnego egzekwowania dostępnych instrumentów prawnych stosowanych wobec strażników dostępu w rozumieniu niniejszego rozporządzenia.
2. W stosownych przypadkach Komisja może konsultować się z organami krajowymi we wszelkich sprawach związanych ze stosowaniem niniejszego rozporządzenia.

*Artykuł 38***Współpraca i koordynacja z właściwymi organami krajowymi egzekwującymi reguły konkurencji**

1. Komisja oraz odpowiedzialne za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwe organy krajowe państw członkowskich współpracują ze sobą i informują się za pośrednictwem Europejskiej Sieci Konkurencji o podejmowanych działaniach w zakresie egzekwowania. Są one uprawnione do przekazywania sobie wszelkich informacji dotyczących kwestii o charakterze faktycznym lub prawnym, w tym informacji poufnych. W przypadku gdy właściwy organ nie jest członkiem Europejskiej Sieci Konkurencji, Komisja dokonuje niezbędnych ustaleń dotyczących współpracy i wymiany informacji w prowadzonych przez te organy sprawach dotyczących egzekwowania niniejszego rozporządzenia i egzekwowania reguł lub przepisów, o których mowa w art. 1 ust. 6. Komisja może ustanowić takie ustalenia w formie wykonawczej, jak określono w art. 46 ust. 1 lit. l).
2. W przypadku gdy odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego zamierza wszcząć w sprawie strażnika dostępu dochodzenie na podstawie reguł lub przepisów krajowych, o których mowa w art. 1 ust. 6, informuje Komisję na piśmie o pierwszej formalnej czynności dochodzeniowej przed jej podjęciem lub niezwłocznie po jej podjęciu. Informację tę można również udostępnić odpowiedzialnym za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwym organom krajowym innych państw członkowskich.
3. W przypadku gdy odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego zamierza nałożyć obowiązki na strażników dostępu na podstawie reguł lub przepisów krajowych, o których mowa w art. 1 ust. 6, przekazuje Komisji projekt środka nie później niż 30 dni przed jego przyjęciem, przedstawiając powody jego wprowadzenia. W przypadku środków tymczasowych odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego przekazuje Komisji projekt planowanego środka tymczasowego jak najszybciej, najpóźniej niezwłocznie po przyjęciu takiego środka. Informację tę można również udostępnić odpowiedzialnym za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwym organom krajowym innych państw członkowskich.
4. Mechanizmy przekazywania informacji określone w ust. 2 i 3 nie mają zastosowania do decyzji przewidzianych na podstawie krajowych przepisów dotyczących łączenia przedsięwzięć.
5. Informacje wymieniane na podstawie ust. 1–3 niniejszego artykułu są wymieniane i wykorzystywane wyłącznie do celów koordynacji egzekwowania niniejszego rozporządzenia oraz reguł i przepisów, o których mowa w art. 1 ust. 6.
6. Komisja może zwrócić się do odpowiedzialnych za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwych organów krajowych państw członkowskich o udzielenie wsparcia w zakresie dowolnego badania rynku przeprowadzanego na podstawie niniejszego rozporządzenia.
7. W przypadku gdy odpowiedzialny za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwy organ krajowy państwa członkowskiego ma na podstawie prawa krajowego odpowiednie kompetencje i uprawnienia dochodzeniowe, może on z własnej inicjatywy przeprowadzić dochodzenie w sprawie możliwego nieprzestrzegania na jego terytorium art. 5, 6 i 7 niniejszego rozporządzenia. Przed podjęciem pierwszej formalnej czynności dochodzeniowej organ ten informuje o tym Komisję na piśmie.



Wszczęcie postępowania przez Komisję na podstawie art. 20 pozbawia odpowiedzialne za egzekwowanie reguł i przepisów, o których mowa w art. 1 ust. 6, właściwe organy krajowe państw członkowskich możliwości przeprowadzenia takiego dochodzenia lub kończy takie dochodzenie, jeżeli jest już ono w toku. Organy te składają Komisji sprawozdanie z ustaleń takiego dochodzenia w celu wsparcia Komisji jako jedyne go organu egzekwującego niniejsze rozporządzenie.

#### Artykuł 39

### Współpraca z sądami krajowymi

1. W postępowaniach dotyczących stosowania niniejszego rozporządzenia sądy krajowe mogą zwrócić się do Komisji o przekazanie informacji będących w jej posiadaniu lub opinii Komisji na temat kwestii dotyczących stosowania niniejszego rozporządzenia.
2. Państwa członkowskie przekazują Komisji kopie wszelkich pisemnych wyroków wydanych przez sądy krajowe w sprawach dotyczących stosowania niniejszego rozporządzenia. Kopie takie przekazywane są niezwłocznie po doręczeniu stronom całości wyroku na piśmie.
3. W przypadku gdy wymaga tego spójne stosowanie niniejszego rozporządzenia Komisja, działając z własnej inicjatywy, może przedkładać pisemne uwagi sądom krajowym. Za zgodą przedmiotowego sądu Komisja może również przedstawiać uwagi ustne.
4. Wyłącznie w celu przygotowania własnych uwag Komisja może zwrócić się z wnioskiem do odpowiedniego sądu krajowego o przekazanie lub zapewnienie przekazania jej wszelkich dokumentów niezbędnych do oceny sprawy.
5. Sądy krajowe nie mogą wydawać decyzji sprzecznych z decyzją przyjętą przez Komisję na podstawie niniejszego rozporządzenia. Sądy krajowe unikają również wydawania decyzji pozostających w sprzeczności z decyzją rozważaną przez Komisję w trakcie postępowania, które wszczęła ona na podstawie niniejszego rozporządzenia. W tym celu sąd krajowy może rozważyć, czy konieczne jest zawieszenie toczącego się przed nim postępowania. Pozostaje to bez uszczerbku dla możliwości wystąpienia przez sądy krajowe z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym na podstawie art. 267 TFUE.

#### Artykuł 40

### Grupa wysokiego szczebla

1. Komisja ustanawia grupę wysokiego szczebla ds. aktu o rynkach cyfrowych (zwaną dalej „grupą wysokiego szczebla”).
2. W skład grupy wysokiego szczebla wchodzi następujące europejskie organy i sieci:
  - a) Organ Europejskich Regulatorów Łączności Elektronicznej,
  - b) Europejski Inspektor Ochrony Danych i Europejska Rada Ochrony Danych,
  - c) Europejska Sieć Konkurencji,
  - d) sieć współpracy w zakresie ochrony konsumenta, oraz
  - e) Europejska Grupa Regulatorów ds. Audiowizualnych Usług Medialnych.
3. Każdy europejski organ i każda europejska sieć, o których mowa w ust. 2, ma w grupie wysokiego szczebla równą liczbę przedstawicieli. Grupa wysokiego szczebla liczy maksymalnie 30 członków.
4. Komisja zapewnia obsługę sekretariatu grupy wysokiego szczebla w celu ułatwienia jej prac. Grupie wysokiego szczebla przewodniczy Komisja, która uczestniczy w posiedzeniach grupy. Grupa wysokiego szczebla zbiera się na wniosek Komisji co najmniej raz na rok kalendarzowy. Komisja zwołuje też posiedzenie grupy na wniosek większości członków wchodzących w jej skład w celu zajęcia się konkretnymi kwestiami.

5. Grupa wysokiego szczebla może służyć Komisji doradztwem i wiedzą fachową w dziedzinach wchodzących w zakres kompetencji jej członków, w tym:

- a) doradztwem i zaleceniami w swojej dziedzinie wiedzy fachowej, mającymi znaczenie dla ogólnych kwestii dotyczących wykonywania lub egzekwowania niniejszego rozporządzenia; lub
- b) doradztwem i wiedzą fachową promującymi spójne podejście regulacyjne w ramach różnych instrumentów regulacyjnych.

6. Grupa wysokiego szczebla może w szczególności identyfikować i oceniać obecne i potencjalne interakcje między niniejszym rozporządzeniem a przepisami sektorowymi stosowanymi przez organy krajowe wchodzące w skład europejskich organów i sieci, o których mowa w ust. 2, i przekazywać Komisji roczne sprawozdanie przedstawiające taką ocenę i identyfikujące potencjalne problemy w zakresie nakładania się regulacji. Takiemu sprawozdaniu mogą towarzyszyć zalecenia mające na celu konwergencję w kierunku spójnych podejść transdyscyplinarnych i synergii między wykonywaniem niniejszego rozporządzenia a innymi rozporządzeniami sektorowymi. Sprawozdanie przekazuje się Parlamentowi Europejskiemu i Radzie.

7. W ramach badań rynku dotyczących nowych usług i nowych praktyk grupa wysokiego szczebla może służyć Komisji wiedzą fachową co do potrzeby zmiany przepisów niniejszego rozporządzenia, dodania nowych przepisów lub uchylenia przepisów niniejszego rozporządzenia w celu zapewnienia contestowalnych i uczciwych rynków cyfrowych w całej Unii.

#### Artykuł 41

### Wniosek o przeprowadzenie badania rynku

1. Trzy państwa członkowskie lub większa ich liczba mogą zwrócić się do Komisji z wnioskiem o rozpoczęcie badania rynku na podstawie art. 17, ponieważ uważają, że istnieją uzasadnione powody, by podejrzewać, że przedsiębiorstwo powinno zostać wskazane jako strażnik dostępu.

2. Jedno państwo członkowskie lub większa ich liczba mogą zwrócić się do Komisji z wnioskiem o rozpoczęcie badania rynku na podstawie art. 18, ponieważ uważają, że istnieją uzasadnione powody, by podejrzewać, że strażnik dostępu systematycznie nie wypełnia co najmniej jednego obowiązku ustanowionego w art. 5, 6 i 7 oraz utrzymał, umocnił lub rozszerzył swoją pozycję strażnika dostępu w odniesieniu do wymogów określonych w art. 3 ust. 1.

3. Trzy państwa członkowskie lub większa ich liczba mogą zwrócić się do Komisji z wnioskiem o przeprowadzenie badania rynku na podstawie art. 19, ponieważ uważają, że istnieją uzasadnione powody, by podejrzewać, że:

- a) do wykazu podstawowych usług platformowych ustanowionego w art. 2 pkt 2 należy dodać jedną usługę świadczoną w sektorze cyfrowym lub większą ich liczbę, lub
- b) niniejsze rozporządzenie nie zaradziło skutecznie określonej praktyce, która może ograniczać contestowalność podstawowych usług platformowych lub być nieuczciwa, lub większej liczbie takich praktyk.

4. Państwa członkowskie przedkładają dowody na poparcie swoich wniosków na podstawie ust. 1, 2 i 3. W przypadku wniosków na podstawie ust. 3 dowody takie mogą obejmować informacje na temat nowo wprowadzonych ofert produktów, usług, oprogramowania lub funkcji, budzących obawy co do contestowalności lub uczciwości, niezależnie od tego, czy są one wdrażane w ramach istniejących podstawowych usług platformowych czy w inny sposób.

5. W terminie 4 miesięcy od otrzymania wniosku na podstawie niniejszego artykułu Komisja ustala, czy istnieją uzasadnione powody, by rozpocząć badanie rynku na podstawie ust. 1, 2 lub 3. Komisja publikuje wyniki swojej oceny.

#### Artykuł 42

### Powództwa przedstawicielskie

Do powództw przedstawicielskich wytaczanych przeciwko strażnikom dostępu za naruszenia przepisów niniejszego rozporządzenia szkodzące lub mogące szkodzić zbiorowym interesom konsumentów stosuje się dyrektywę (UE) 2020/1828.

*Artykuł 43***Zgłaszanie naruszeń i ochrona osób dokonujących zgłoszeń**

Do zgłaszania naruszeń niniejszego rozporządzenia i do ochrony osób zgłaszających takie naruszenia stosuje się dyrektywę (UE) 2019/1937.

## ROZDZIAŁ VI

**PRZEPISY KOŃCOWE***Artykuł 44***Publikacja decyzji**

1. Komisja publikuje decyzje, które podejmuje na podstawie art. 3 i 4, art. 8 ust. 2, art. 9, 10, 16–20 i 24, art. 25 ust. 1, art. 29, 30 i 31. Taka publikacja zawiera wskazanie stron i najważniejsze elementy decyzji, w tym ewentualnie nałożone sankcje.
2. Publikacji dokonuje się z poszanowaniem uzasadnionego interesu strażników dostępu lub osób trzecich w zakresie ochrony ich informacji poufnych.

*Artykuł 45***Kontrola ze strony Trybunału Sprawiedliwości**

Zgodnie z art. 261 TFUE Trybunał Sprawiedliwości ma nieograniczone prawo orzekania w zakresie kontroli decyzji, którymi Komisja nałożyła grzywny lub okresowe kary pieniężne. Trybunał Sprawiedliwości może uchylić, obniżyć lub podwyższyć nałożoną grzywnę lub okresową karę pieniężną.

*Artykuł 46***Przepisy wykonawcze**

1. Komisja może przyjmować akty wykonawcze ustanawiające szczegółowe zasady w odniesieniu do:
  - a) formy, treści i innych szczegółów powiadomień i przekazywanych informacji na podstawie art. 3;
  - b) formy, treści i innych szczegółów środków technicznych, które strażnicy dostępu wdrażają w celu zapewnienia zgodności z art. 5, 6 lub 7;
  - c) ustaleń operacyjnych i technicznych służących wdrożeniu interoperacyjności usług łączności interpersonalnej niewykorzystujących numerów na podstawie art. 7;
  - d) formy, treści i innych szczegółów uzasadnionego wniosku na podstawie art. 8 ust. 3;
  - e) formy, treści i innych szczegółów uzasadnionych wniosków na podstawie art. 9 i 10;
  - f) formy, treści i innych szczegółów obowiązkowych sprawozdań przedkładanych na podstawie art. 11;
  - g) metodyki i procedury dotyczące poddanego audytowi opisu technik wykorzystywanych do profilowania konsumentów, o którym to opisie mowa w art. 15 ust. 1; opracowując w tym celu projekt aktu wykonawczego, Komisja konsultuje się z Europejskim Inspektorem Ochrony Danych i może konsultować się z Europejską Radą Ochrony Danych, społeczeństwem obywatelskim i innymi odpowiednimi ekspertami;
  - h) formy, treści i innych szczegółów powiadomień i przekazywanych informacji na podstawie art. 14 i 15;

- i) praktycznych ustaleń w odniesieniu do postępowań dotyczących badań rynku przeprowadzanych na podstawie art. 17, 18 i 19 oraz w odniesieniu do postępowań przeprowadzanych na podstawie art. 24, 25 i 29;
- j) praktycznych ustaleń dotyczących wykonywania prawa do bycia wysłuchanym przewidzianego w art. 34;
- k) praktycznych ustaleń dotyczących warunków ujawnienia przewidzianego w art. 34;
- l) praktycznych ustaleń dotyczących współpracy i koordynacji między Komisją a organami krajowymi przewidzianych w art. 37 i 38; oraz
- m) praktycznych ustaleń dotyczących obliczania i przedłużania terminów.

2. Akty wykonawcze, o których mowa w ust. 1 lit. a) – k) i lit. m) niniejszego artykułu, przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 50 ust. 2.

Akt wykonawczy, o którym mowa w ust. 1 lit. l) niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 50 ust. 3.

3. Przed przyjęciem aktu wykonawczego na podstawie ust. 1 Komisja publikuje jego projekt i zaprasza wszystkie zainteresowane strony do przedłożenia uwag w wyznaczonym terminie, który nie może być krótszy niż jeden miesiąc.

#### Artykuł 47

#### Wytyczne

Komisja może przyjmować wytyczne dotyczące wszelkich aspektów niniejszego rozporządzenia w celu ułatwienia jego skutecznego wykonania i egzekwowania.

#### Artykuł 48

#### Normalizacja

W stosownych i koniecznych przypadkach Komisja może upoważnić europejskie organy normalizacyjne do opracowania odpowiednich norm ułatwiających wypełnianie obowiązków określonych w niniejszym rozporządzeniu.

#### Artykuł 49

#### 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. 3 ust. 6 i 7 i art. 12 ust. 1, 3 i 4, powierza się Komisji na okres pięciu lat od dnia 1 listopada 2022 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.
3. Przekazanie uprawnień, o którym mowa w art. 3 ust. 6 i 7 i art. 12 ust. 1, 3 i 4, 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. 3 ust. 6 i 7 i art. 12 ust. 1, 3 i 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch 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 dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

#### Artykuł 50

##### **Procedura komitetowa**

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

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 4 rozporządzenia (UE) nr 182/2011.

W przypadku gdy opinia komitetu ma zostać uzyskana w drodze procedury pisemnej, procedura ta kończy się bez osiągnięcia rezultatu, gdy – przed upływem terminu na wydanie opinii – zdecyduje o tym przewodniczący komitetu lub wniesie o to zwykła większość członków komitetu.

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

4. Komisja przekazuje opinię komitetu adresatowi danej decyzji wraz z tą decyzją. Komisja podaje do publicznej wiadomości tę opinię wraz z daną decyzją, uwzględniając uzasadniony interes w zakresie ochrony tajemnicy zawodowej.

#### Artykuł 51

##### **Zmiana dyrektywy (UE) 2019/1937**

W pkt J części I załącznika do dyrektywy (UE) 2019/1937 dodaje się podpunkt w brzmieniu:

„(iv) 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 21.9.2022, s. 1).”.

#### Artykuł 52

##### **Zmiana dyrektywy (UE) 2020/1828**

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

„67) 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 21.9.2022, s. 1).”.

#### Artykuł 53

##### **Przegląd**

1. Do dnia 3 maja 2026 r., a następnie co trzy lata, Komisja dokona oceny niniejszego rozporządzenia i przedstawi sprawozdanie Parlamentowi Europejskiemu, Radzie i Europejskiemu Komitetowi Ekonomiczno-Społecznemu.

2. W ramach ocen sprawdza się, czy osiągnięto cele niniejszego rozporządzenia polegające na zapewnieniu kontestowalnych i uczciwych rynków, oraz określa się wpływ niniejszego rozporządzenia na użytkowników biznesowych, w szczególności MŚP, i na użytkowników końcowych. Ponadto Komisja ocenia, czy można rozszerzyć zakres stosowania art. 7 na internetowe serwisy społecznościowe.
3. W ramach ocen ustala się, czy w celu zapewnienia kontestowalnych i uczciwych rynków cyfrowych w całej Unii konieczna jest zmiana przepisów, w tym dotyczących wykazu podstawowych usług platformowych ustanowionego w art. 2 pkt 2, a także obowiązków ustanowionych w art. 5, 6 i 7 i ich egzekwowania. Po przeprowadzeniu ocen Komisja podejmuje stosowne działania, które mogą obejmować wnioski ustawodawcze.
4. Właściwe organy państw członkowskich dostarczają wszelkie będące w ich posiadaniu istotne informacje, jakich Komisja może potrzebować do celów sporządzenia sprawozdania, o którym mowa w ust. 1.

#### Artykuł 54

#### Wejście w życie i stosowanie

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

Niniejsze rozporządzenie stosuje się od dnia 2 maja 2023 r.

Jednakże art. 3 ust. 6 i 7 oraz art. 40, 46, 47, 48, 49 i 50 stosuje się od dnia 1 listopada 2022 r., a art. 42 i 43 stosuje się od dnia 25 czerwca 2023 r.

Niemniej jednak, jeżeli data 25 czerwca 2023 r. poprzedza datę rozpoczęcia stosowania, o której mowa w akapicie drugim niniejszego artykułu, stosowanie art. 42 i art. 43 zostaje odroczone do daty rozpoczęcia stosowania, o której mowa w akapicie drugim niniejszego artykułu.

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

Sporządzono w Strasburgu dnia 14 września 2022 r.

W imieniu Parlamentu Europejskiego  
Przewodnicząca  
R. METSOLA

W imieniu Rady  
Przewodniczący  
M. BEK

## ZAŁĄCZNIK

## A. Uwagi ogólne

1. Celem niniejszego załącznika jest określenie metodyki identyfikacji i obliczania „aktywnych użytkowników końcowych” i „aktywnych użytkowników biznesowych” dla każdej podstawowej usługi platformowej wymienionej w art. 2 pkt 2. Stanowi on punkt odniesienia umożliwiający przedsiębiorstwu ocenę, czy jego podstawowe usługi platformowe osiągnęły progi ilościowe określone w art. 3 ust. 2 lit. b), w związku z czym zachodzi domniemanie, że spełniają warunek określony w art. 3 ust. 1 lit. b). Taki punkt odniesienia będzie zatem równie istotny dla każdej szerszej oceny przeprowadzanej na podstawie art. 3 ust. 8. Obowiązkiem przedsiębiorstwa jest obliczenie liczby wspomnianych użytkowników z najdokładniejszym przybliżeniem, zgodnie ze wspólnymi zasadami i szczegółową metodyką przedstawioną w niniejszym załączniku. Żaden z elementów niniejszego załącznika nie pozbawia Komisji, w ramach terminów określonych w odpowiednich przepisach niniejszego rozporządzenia, możliwości żądania od przedsiębiorstwa świadczącego podstawowe usługi platformowe dostarczenia informacji niezbędnych do identyfikacji i obliczenia „aktywnych użytkowników końcowych” i „aktywnych użytkowników biznesowych”. Żaden z elementów niniejszego załącznika nie powinien stanowić podstawy prawnej do śledzenia użytkowników. Metodyka zawarta w niniejszym załączniku pozostaje bez uszczerbku dla obowiązków ustanowionych w niniejszym rozporządzeniu, a mianowicie obowiązków w art. 3 ust. 3 i 8 oraz w art. 13 ust. 3. W szczególności wymagane przestrzeganie art. 13 ust. 3 oznacza również identyfikowanie i obliczanie „aktywnych użytkowników końcowych” i „aktywnych użytkowników biznesowych” w oparciu o dokładny pomiar albo najdokładniejsze dostępne przybliżenie zgodnie z faktycznymi zdolnościami w zakresie identyfikacji i obliczania, którymi w danym momencie dysponuje przedsiębiorstwo świadczące podstawowe usługi platformowe. Pomiary te lub najdokładniejsze dostępne przybliżenie muszą być spójne z danymi przekazywanymi na podstawie art. 15 i obejmować te dane.
2. W art. 2 pkt 20 i 21 określono definicje „użytkownika końcowego” i „użytkownika biznesowego”, wspólne dla wszystkich podstawowych usług platformowych.
3. W celu identyfikacji i obliczenia liczby „aktywnych użytkowników końcowych” i „aktywnych użytkowników biznesowych” w niniejszym załączniku stosuje się pojęcie „unikalnego użytkownika”. Pojęcie „unikalnego użytkownika” obejmuje „aktywnych użytkowników końcowych” i „aktywnych użytkowników biznesowych” liczonych tylko raz w odniesieniu do danej podstawowej usługi platformowej w określonym okresie (tzn. w okresie miesiąca w przypadku „aktywnych użytkowników końcowych” i w okresie roku w przypadku „aktywnych użytkowników biznesowych”), niezależnie od tego, ile razy w tym okresie użytkownicy ci weszli w interakcję z odpowiednią podstawową usługą platformową. Pozostaje to bez uszczerbku dla faktu, że ta sama osoba fizyczna lub prawna może jednocześnie być „aktywnym użytkownikiem końcowym” i „aktywnym użytkownikiem biznesowym” różnych podstawowych usług platformowych.

## B. „Aktywni użytkownicy końcowi”

1. Liczbę „unikalnych użytkowników” w odniesieniu do „aktywnych użytkowników końcowych” identyfikuje się zgodnie z najdokładniejszym miernikiem podanym przez przedsiębiorstwo świadczące którąkolwiek z podstawowych usług platformowych, w szczególności:
  - a. Uznaje się, że zbieranie danych na temat korzystania z podstawowych usług platformowych w oparciu o środowiska logowania jednorazowego lub stałego (środowiska *signed-in* lub *logged-in*) stwarza *prima facie* najmniejsze ryzyko wielokrotnego liczenia tego samego użytkownika, na przykład w związku z korzystaniem przez użytkowników z różnych urządzeń lub platform. Przedsiębiorstwo przedkłada zatem zagregowane zanonimizowane dane dotyczące liczby unikalnych użytkowników końcowych dla danej podstawowej usługi platformowej w oparciu o środowiska logowania jednorazowego lub stałego, jeżeli takie dane istnieją.
  - b. W przypadku podstawowych usług platformowych, do których użytkownicy końcowi mają również dostęp poza środowiskami logowania jednorazowego lub stałego, przedsiębiorstwo dodatkowo przedkłada zagregowane zanonimizowane dane na temat liczby unikalnych użytkowników końcowych danej podstawowej usługi platformowej w oparciu o alternatywny miernik ujmujący również użytkowników końcowych spoza środowisk logowania jednorazowego lub stałego; miernikami takimi mogą być na przykład adresy IP, identyfikatory plików cookie lub inne identyfikatory, takie jak identyfikatory RFID (identyfikacja za pomocą fal radiowych), pod warunkiem że te adresy lub identyfikatory są obiektywnie niezbędne do świadczenia podstawowych usług platformowych.
2. Liczba „użytkowników końcowych aktywnych miesięcznie” oparta jest na średniej liczbie użytkowników końcowych aktywnych miesięcznie w okresie obejmującym przeważającą część roku obrotowego. Pojęcie „przeważającej części roku obrotowego” ma na celu umożliwienie przedsiębiorstwu świadczącemu podstawowe usługi platformowe pominięcia wartości odstających w danym roku. Wartości odstające co do zasady oznaczają dane liczbowe znacznie wykra-

czające poza standardowe i przewidywalne wartości. Przykładem tego, co może stanowić takie wartości odstające, jest nieprzewidziany wzrost lub spadek interakcji użytkowników z usługą, który miał miejsce w ciągu jednego miesiąca danego roku obrotowego. Wartościami odstającymi nie są dane liczbowe dotyczące wydarzeń powtarzających się co roku, takich jak coroczne promocje sprzedaży.

#### C. „Aktywni użytkownicy biznesowi”

Liczbę „unikalnych użytkowników” w odniesieniu do „aktywnych użytkowników biznesowych” należy ustalać, w stosownych przypadkach, z wykorzystaniem poziomu konta użytkownika, gdzie każde odrębne konto biznesowe powiązane z korzystaniem z podstawowej usługi platformowej świadczonej przez przedsiębiorstwo oznacza unikalnego użytkownika biznesowego danej podstawowej usługi platformowej. Jeżeli pojęcie „konta biznesowego” nie dotyczy danej podstawowej usługi platformowej, przedsiębiorstwo świadczące podstawowe usługi platformowe ustala liczbę unikalnych użytkowników biznesowych poprzez odniesienie do danego przedsiębiorstwa.

#### D. Przekazywanie informacji

1. Przedsiębiorstwo przekazujące Komisji na podstawie art. 3 ust. 3 informacje dotyczące liczby aktywnych użytkowników końcowych i aktywnych użytkowników biznesowych danej podstawowej usługi platformowej jest odpowiedzialne za zapewnienie kompletności i dokładności tych informacji. W związku z tym:

- a. Przedsiębiorstwo jest odpowiedzialne za przekazywanie danych dotyczących danej podstawowej usługi platformowej w sposób niepowodujący zaniżenia lub zawyżenia liczby aktywnych użytkowników końcowych i aktywnych użytkowników biznesowych (na przykład gdy użytkownicy uzyskują dostęp do podstawowych usług platformowych z wykorzystaniem różnych platform lub urządzeń).
- b. Przedsiębiorstwo jest odpowiedzialne za dostarczenie dokładnych i zwięzłych wyjaśnień co do metodyki stosowanej w celu ustalenia informacji i za ryzyko zaniżenia lub zawyżenia liczby aktywnych użytkowników końcowych i aktywnych użytkowników biznesowych danej podstawowej usługi platformowej oraz za rozwiązania przyjęte w celu wyeliminowania tego ryzyka.
- c. Przedsiębiorstwo dostarcza danych opartych na alternatywnym mierniku, w przypadku gdy Komisja ma wątpliwości co do dokładności danych dostarczonych przez przedsiębiorstwo świadczące podstawowe usługi platformowe.

2. Do celów obliczania liczby „aktywnych użytkowników końcowych” i „aktywnych użytkowników biznesowych”:

- a. Przedsiębiorstwo świadczące podstawowe usługi platformowe nie identyfikuje podstawowych usług platformowych należących do tej samej kategorii podstawowych usług platformowych na podstawie art. 2 pkt 2 jako odrębne usługi, opierając się głównie na fakcie, że świadczone są one z wykorzystaniem różnych nazw domen – czy to krajowych domen najwyższego poziomu (ccTLD), czy funkcjonalnych domen najwyższego poziomu (gTLD) – ani z uwagi na jakiegokolwiek atrybuty geograficzne.
- b. Przedsiębiorstwo świadczące podstawowe usługi platformowe uznaje za odrębne te podstawowe usługi platformowe, które wykorzystywane są do różnych celów przez ich użytkowników końcowych lub ich użytkowników biznesowych albo przez obie te grupy, nawet w przypadku gdy ich użytkownicy końcowi lub użytkownicy biznesowi mogą być ci sami i nawet w przypadku gdy usługi te należą do tej samej kategorii podstawowych usług platformowych na podstawie art. 2 pkt 2.
- c. Przedsiębiorstwo świadczące podstawowe usługi platformowe uznaje za odrębne te podstawowe usługi platformowe, które są przez nie oferowane w sposób zintegrowany, ale które:
  - (i) nie należą do tej samej kategorii podstawowych usług platformowych na podstawie art. 2 pkt 2 lub
  - (ii) wykorzystywane są do różnych celów przez ich użytkowników końcowych lub ich użytkowników biznesowych albo przez obie te grupy, nawet w przypadku gdy ich użytkownicy końcowi lub użytkownicy biznesowi mogą być ci sami i nawet w przypadku gdy usługi te należą do tej samej kategorii podstawowych usług platformowych na podstawie art. 2 pkt 2.

#### E. Szczegółowe definicje

Poniższa tabela zawiera szczegółowe definicje „aktywnych użytkowników końcowych” i „aktywnych użytkowników biznesowych” dla każdej podstawowej usługi platformowej.



Podstawowe usługi platformowe	Aktywni użytkownicy końcowi	Aktywni użytkownicy biznesowi
Usługi pośrednictwa internetowego	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu weszli w interakcję z usługą pośrednictwa internetowego, na przykład poprzez aktywne zalogowanie się, dokonanie zapytania, kliknięcie lub przewijanie, lub którzy co najmniej raz w miesiącu dokonali transakcji, korzystając z usługi pośrednictwa internetowego.	Liczba unikalnych użytkowników biznesowych, którzy w ciągu całego roku dysponowali co najmniej jedną pozycją w ramach usługi pośrednictwa internetowego lub którzy co najmniej raz w miesiącu dokonali transakcji, korzystając z usługi pośrednictwa internetowego.
Wyszukiwarki internetowe	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu weszli w interakcję z wyszukiwarką internetową, na przykład poprzez dokonanie zapytania.	Liczba unikalnych użytkowników biznesowych posiadających profesjonalną witrynę internetową (tj. stronę internetową wykorzystywaną w celach komercyjnych lub zawodowych), która w ciągu roku została zaindeksowana lub znajdowała się w indeksie.
Internetowe serwisy społecznościowe	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu weszli w interakcję z internetowym serwisem społecznościowym, na przykład poprzez aktywne zalogowanie się, otwarcie strony, przewijanie, klikanie, polubienie, dokonanie zapytania, zamieszczenie wpisu lub przesłanie komentarza.	Liczba unikalnych użytkowników biznesowych, którzy w ramach internetowego serwisu społecznościowego dysponują pozycją lub kontem biznesowym i którzy co najmniej raz w roku weszli w interakcję z internetowym serwisem społecznościowym, na przykład poprzez aktywne zalogowanie się, otwarcie strony, przewijanie, klikanie, zareagowanie, dokonanie zapytania, zamieszczenie wpisu lub przesłanie komentarza, lub korzystanie z narzędzi dla przedsiębiorstw oferowanych przez serwis.
Usługi platformy udostępniania wideo	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu weszli w interakcję z usługą platformy udostępniania wideo, na przykład poprzez odtworzenie fragmentu treści audiowizualnych, dokonanie zapytania lub zamieszczenie materiału z treściami audiowizualnymi, w tym w szczególności wideo zamieszczanych przez użytkowników.	Liczba unikalnych użytkowników biznesowych, którzy w ciągu roku dostarczyli co najmniej jeden materiał z treściami audiowizualnymi w celu zamieszczenia lub odtworzenia w ramach usługi platformy udostępniania wideo.
Usługi łączności interpersonalnej niewykorzystujące numerów	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu zainicjowali komunikację za pośrednictwem usługi łączności interpersonalnej niewykorzystującej numerów lub w jakikolwiek sposób uczestniczyli w takiej komunikacji.	Liczba unikalnych użytkowników biznesowych, którzy co najmniej raz w roku skorzystali z konta biznesowego lub w inny sposób zainicjowali komunikację za pośrednictwem usługi łączności interpersonalnej niewykorzystującej numerów lub w jakikolwiek sposób uczestniczyli w takiej komunikacji, by w sposób bezpośredni komunikować się z użytkownikiem końcowym.
Systemy operacyjne	Liczba unikalnych użytkowników końcowych korzystających z urządzenia z systemem operacyjnym, który uruchomiono, zaktualizowano lub wykorzystano co najmniej raz w miesiącu.	Liczba unikalnych programistów, którzy w ciągu roku opublikowali, zaktualizowali lub zaoferowali co najmniej jedną aplikację lub program wykorzystujące język programowania lub jakiekolwiek narzędzia programistyczne systemu operacyjnego lub w jakikolwiek sposób działające w tym systemie operacyjnym.

Podstawowe usługi platformowe	Aktywni użytkownicy końcowi	Aktywni użytkownicy biznesowi
Wirtualny asystent	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu w jakikolwiek sposób weszli w interakcję z wirtualnym asystentem, na przykład poprzez jego aktywację, zadanie pytania, uzyskanie dostępu do usługi poprzez wydanie polecenia lub sterowanie inteligentnym urządzeniem domowym.	Liczba unikalnych programistów, którzy w ciągu roku zaoferowali co najmniej jedną aplikację wirtualnego asystenta lub funkcjonalność umożliwiającą dostęp do istniejącej aplikacji za pośrednictwem wirtualnego asystenta.
Przeglądarki internetowe	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu weszli w interakcję z wyszukiwarką internetową, na przykład poprzez zamieszczenie zapytania lub adresu strony internetowej w polu URL wyszukiwarki internetowej.	Liczba unikalnych użytkowników biznesowych, do których profesjonalnych stron internetowych (tj. stron internetowych wykorzystywanych w celach komercyjnych lub zawodowych) co najmniej raz w ciągu roku uzyskano dostęp za pośrednictwem przeglądarki internetowej lub którzy w ciągu roku zaoferowali wtyczkę, rozszerzenie lub dodatki dla przeglądarki internetowej.
Usługi przetwarzania w chmurze	Liczba unikalnych użytkowników końcowych, którzy co najmniej raz w miesiącu weszli w interakcję z jakąkolwiek usługą przetwarzania w chmurze pochodzącą od odnośnego dostawcy usług przetwarzania w chmurze w zamian za jakikolwiek rodzaj wynagrodzenia, niezależnie od tego, czy wynagrodzenie to ma miejsce w tym samym miesiącu.	Liczba unikalnych użytkowników biznesowych, którzy w ciągu roku świadczyli jakąkolwiek usługę przetwarzania w chmurze opartą na infrastrukturze chmury odnośnego dostawcy usług przetwarzania w chmurze.
Internetowe usługi reklamowe	W przypadku sprzedaży na własny rachunek przestrzeni reklamowych: liczba unikalnych użytkowników końcowych, którym co najmniej raz w miesiącu zaprezentowano reklamę. W przypadku usług pośrednictwa reklamowego (w tym sieci reklamowych, giełd reklamowych i wszelkich innych usług pośrednictwa w zakresie reklamy): liczba unikalnych użytkowników końcowych, którym co najmniej raz w miesiącu zaprezentowano reklamę, co doprowadziło do aktywacji usługi pośrednictwa reklamowego.	W przypadku sprzedaży na własny rachunek przestrzeni reklamowych: liczba unikalnych reklamodawców, których reklama została wyświetlona co najmniej raz w roku. W przypadku usług pośrednictwa reklamowego (w tym sieci reklamowych, giełd reklamowych i wszelkich innych usług pośrednictwa w zakresie reklamy): liczba unikalnych użytkowników biznesowych (w tym reklamodawców, wydawców lub innych pośredników), którzy w ciągu roku weszli w interakcję z usługą pośrednictwa reklamowego lub byli w ramach takiej usługi obsługiwani.