KOMISJA
EUROPEJSKA

Bruksela, dnia 17.9.2026 r.
COM(2026) 681 final

2026/0286 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

EU KIDS ACT – „UE na straży odpowiedzialnych i godnych zaufania przestrzeni cyfrowych w internecie”

{SWD(2026) 681 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Tylko połowa dzieci w wieku 9–16 lat w całej Europie twierdzi, że czuje się bezpiecznie w internecie. Zagrożenia, na jakie narażeni są małoletni w internecie, mają realny i pilny charakter. Wpływają na zdrowie, rozwój i dobrostan małoletnich, powodując np. ograniczenie aktywności fizycznej, zwiększone ryzyko krótkowzroczności i ograniczenie snu, objawy depresyjne i lękowe, obniżenie samooceny, negatywny wpływ na uczenie się i rozwój poznawczy, zaburzenia odżywiania, zmniejszoną empatię, samotność i zachowania uzależniające. Małoletni w internecie są również narażeni na ryzyko cyberszykanowania, niegodziwego traktowania w celach seksualnych i nagabywania w celach seksualnych.

Ochrona małoletnich w internecie jest jednym z priorytetów politycznych Komisji. W orędziu o stanie Unii w 2025 r. przewodnicząca Komisji Ursula von der Leyen ogłosiła, że zleci zespołowi ekspertów doradzanie jej w sprawie najlepszego podejścia do bezpieczeństwa dzieci w internecie w Europie. W wyniku działań podjętych w pierwszej połowie 2026 r. z udziałem szerokiego grona ekspertów z różnych dziedzin, a także przedstawicieli przemysłu, rodziców i młodzieży, współprzewodniczący specjalnego panelu przedstawili swoje zalecenia przewodniczącej w lipcu 2026 r. W zaleceniach określono jasną ścieżkę poprawy bezpieczeństwa małoletnich w internecie i zapewnienia funkcjonowania jednolitego rynku. W szczególności zalecono ogólnounijne ograniczenie dostępu, zharmonizowane zasady uwzględniania bezpieczeństwa na etapie projektowania, a także proporcjonalne, chroniące prywatność systemy potwierdzania wieku. Ponadto zalecono uwzględnienie usług cyfrowych wykraczających poza platformy mediów społecznościowych, w tym sklepów z aplikacjami, towarzyszy AI oraz niektórych gier wideo i platform udostępniania wideo oferujących ryzykowne funkcje.

W październiku 2025 r. w deklaracji z Jutlandii podpisanej przez 25 państw członkowskich wezwano do weryfikacji wieku i stworzenia bezpieczniejszego środowiska internetowego dla małoletnich. W konkluzjach z marca 2026 r. i października 2025 r. Rada Europejska podkreśliła również znaczenie ochrony małoletnich w internecie, w tym za pośrednictwem pełnoletności cyfrowej. W sprawozdaniu z listopada 2025 r. w sprawie ochrony małoletnich w internecie Parlament Europejski wezwał do ustanowienia zharmonizowanego europejskiego limitu wieku dojrzałości cyfrowej wynoszącego 16 lat, poniżej którego dostęp do mediów społecznościowych, platform udostępniania wideo i towarzyszy AI nie będzie dozwolony, chyba że za zgodą rodziców lub opiekunów dzieci. Parlament Europejski wezwał również do ustanowienia ujednoliconego europejskiego wieku dojrzałości cyfrowej wynoszącego 13 lat, poniżej którego małoletni nie mogą mieć dostępu do platform mediów społecznościowych. Parlament Europejski uznał również potrzebę wprowadzenia dodatkowych przepisów dotyczących projektowania dostosowanego do wieku i uwzględniania bezpieczeństwa na etapie projektowania. Ponadto wezwał do przyjęcia europejskiego podejścia do potwierdzania wieku zapewniającego pewność prawa.

W całej Unii Europejskiej państwa członkowskie omawiają lub proponują przepisy krajowe mające na celu zwiększenie bezpieczeństwa małoletnich w internecie. Włochy, Francja, Norwegia, Grecja, Austria, Polska i Belgia zgłosiły w 2025 i 2026 r. projekty przepisów ograniczających dostęp małoletnich poniżej pewnego wieku do niektórych usług cyfrowych. Norwegia również powiadomiła o swoich przepisach w maju 2026 r. W prawie wszystkich pozostałych państwach członkowskich konsultacje są w toku, projekty są omawiane

w parlamentach narodowych lub zostały ogłoszone przez rządy. Proponowane projekty przepisów krajowych różnią się pod względem zakresu, limitów wiekowych i rodzajów nałożonych ograniczeń, co grozi fragmentacją jednolitego rynku, zmniejszeniem pewności prawa i zwiększeniem kosztów przestrzegania przepisów, jednocześnie powodując nierówny poziom ochrony małoletnich w całej Unii Europejskiej.

Obecne środowisko internetowe nie jest zaprojektowane z myślą o małoletnich. Chociaż istnieją już przepisy mające na celu stworzenie bezpieczniejszego środowiska internetowego, nie istnieją żadne jednolite przepisy, które traktowałyby dzieci i ich bezpieczeństwo i upodmiotowienie jako punktu wyjścia. Opierając się na kluczowych zasadach określonych w rozporządzeniu (UE) 2022/2065 i rozporządzeniu (UE) 2024/1689, niniejszy wniosek ma na celu ochronę małoletnich przed ryzykownymi usługami cyfrowymi i systemami AI, utrzymanie jednolitego rynku cyfrowego oraz zachowanie spójnych ram regulacyjnych i struktury egzekwowania prawa w celu ochrony małoletnich w internecie.

We wniosku uznaje się ryzyko, na jakie narażeni są małoletni w niektórych internetowych serwisach społecznościowych i platformach udostępniania wideo, i w związku z tym ogranicza się możliwość samodzielnego tworzenia kont w tych konkretnych platformach i systemach przez dzieci w wieku poniżej 15 lat. Poprzez wprowadzenie jednego rozwiązania dotyczącego wieku w całej Unii Europejskiej, wniosek harmonizuje rozbieżne przepisy krajowe, usuwając przeszkody we wdrażaniu jednolitego rynku cyfrowego i zapewniając pewność prawa i podobny poziom ochrony wszystkim dzieciom w Unii Europejskiej. Zostało to połączone z przepisami uznającymi rolę rodziców i opiekunów prawnych we wspieraniu bezpiecznego rozwoju małoletnich w internecie poprzez tworzenie kont o ograniczonych funkcjach dla małoletnich od 13. roku życia, a także z przepisami mającymi na celu stworzenie środowiska bezpiecznych usług i systemów dla bardzo małych dzieci pod ścisłym nadzorem rodzicielskim, uwzględniającymi ich rozwój. Zgodnie z opartym na rozwoju podejściem zalecanym przez współprzewodniczących specjalnego panelu ds. bezpieczeństwa dzieci w internecie małoletni poniżej 13. roku życia nie powinni mieć dostępu do szkodliwych internetowych serwisów społecznościowych i usług platformy udostępniania wideo.

We wniosku określono jasne wymogi uwzględniania bezpieczeństwa na etapie projektowania dla internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz sklepów z aplikacjami. Opierając się na zaleceniach współprzewodniczących specjalnego panelu, wniosek harmonizuje i rozszerza te wymogi, zapewniając pewność prawa na całym jednolitym rynku cyfrowym oraz wysoki poziom ochrony małoletnich w środowisku cyfrowym, biorąc pod uwagę stale zmieniający się charakter modeli biznesowych w tej dynamicznej dziedzinie oraz konieczność uniknięcia luk prawnych.

Aby wesprzeć odroczenie dostępu i wdrożenie wymogów uwzględniania bezpieczeństwa na etapie projektowania, we wniosku ustanowiono jasne ramy potwierdzania wieku wraz z przejrzystymi kryteriami i zabezpieczeniami dotyczącymi stosowania i wdrażania takich systemów. Wprowadzając wymogi dotyczące stosowania metod potwierdzania wieku, wniosek zapewnia, aby stosowanie to było proporcjonalne, skuteczne, wiarygodne i chroniące prywatność. We wniosku przewidziano również wspólne kryteria potwierdzania wieku zapewniające funkcjonowanie jednolitego rynku.

Szybkie, skuteczne i solidne egzekwowanie przepisów ma kluczowe znaczenie dla ochrony małoletnich w internecie i funkcjonowania jednolitego rynku. W związku z tym we wniosku

określono ramy egzekwowania prawa, które opierają się na istniejących strukturach egzekwowania prawa, a jednocześnie przewidziano przyspieszone postępowanie egzekucyjne.

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

Wniosek opiera się na istniejących ramach prawnych dotyczących ochrony małoletnich w internecie, zapewniających funkcjonowanie jednolitego rynku. Opierając się na rozporządzeniu (UE) 2022/2065 i rozporządzeniu (UE) 2024/1689, wniosek zapewnia ciągłość i spójność z unijnymi ramami regulacyjnymi dotyczącymi usług cyfrowych i systemów AI, a jednocześnie wprowadza szczegółowe wymogi dotyczące ochrony małoletnich w internecie, uwzględniając jako punkt wyjścia ich zmieniające się zdolności, bezpieczeństwo i sprawczość.

Proponowane rozporządzenie pozostaje bez uszczerbku dla aktu o usługach cyfrowych i opiera się na określonych w nim przepisach, w szczególności na art. 28 dotyczącym spoczywającego na niektórych dostawcach platform internetowych obowiązku wprowadzenia odpowiednich środków w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich. W proponowanym instrumencie, w szczególności w jego przepisach dotyczących uwzględniania bezpieczeństwa na etapie projektowania, określono w „prawie twardym" te specyfikacje, które Komisja uwzględniła już w wytycznych dotyczących ochrony małoletnich na podstawie rozporządzenia (UE) 2022/2065. W ten sposób ustanowiono w nim obowiązki zdefiniowane w art. 28 rozporządzenia (UE) 2022/2065, w przypadku gdy dotyczą one wymogów uwzględniania bezpieczeństwa na etapie projektowania i potwierdzania wieku. W związku z tym nie ma to wpływu na toczące się sprawy związane z tymi obowiązkami wynikającymi z rozporządzenia (UE) 2022/2065, w szczególności z art. 28. Proponowane rozporządzenie pozostaje również bez uszczerbku dla rozporządzenia (UE) 2024/1689 i opiera się na jego ramach, w szczególności na jego kompleksowych przepisach opartych na analizie ryzyka. Proponowane rozporządzenie ma charakter uzupełniający i nie ma wpływu na zakazy oraz inne obowiązki i wymogi dotyczące systemów AI i modeli AI ogólnego przeznaczenia ustanowione już w rozporządzeniu (UE) 2024/1689.

Strategia na rzecz lepszego internetu dla dzieci (BIK+) wspiera wdrażanie tych ram prawnych, w szczególności rozporządzenia (UE) 2022/2065. Na podstawie BIK+ współfinansowana przez UE sieć centrów bezpieczniejszego internetu oferuje sesje szkoleniowe, telefony zaufania i infolinie oraz prowadzi działania informacyjne. W ramach tej sieci regularnie zasięga się opinii dzieci i młodzieży na temat ich potrzeb i bezpieczeństwa w internecie. W lutym 2026 r. Komisja przyjęła plan działania przeciwko cyberszykanowaniu, aby zapobiec cyberszykanowaniu, zwiększyć świadomość i ułatwić zgłaszanie przypadków cyberszykanowania oraz zapewnić ofiarom odpowiednie wsparcie. Wniosek jest spójny z tymi działaniami o charakterze nieustawodawczym i opiera się na nich, aby zapewnić dzieciom w Europie najlepsze wsparcie podczas korzystania ze środowiska internetowego.

- **Spójność z innymi politykami Unii**

Proponowane rozporządzenie wprowadza horyzontalne ramy ochrony małoletnich w internecie. Niniejsze rozporządzenie pozostaje bez uszczerbku dla przepisów określonych w innych aktach prawnych Unii regulujących inne aspekty świadczenia usług pośrednich na rynku wewnętrznym, w szczególności przepisów dotyczących audiowizualnych usług medialnych, ochrony konsumentów i bezpieczeństwa produktów oraz ochrony danych osobowych.

Wniosek zostanie uzupełniony dalszymi działaniami, które byłyby w pełni zgodne z niniejszym rozporządzeniem, w tym trwającą oceną i zbliżającym się przeglądem dyrektywy o audiowizualnych usługach medialnych, w których dodatkowo uwzględniona zostanie ochrona małoletnich jako widzów i które zapewnią małoletnim wystarczającą ochronę podczas oglądania treści audiowizualnych. Biorąc pod uwagę nowe zagrożenia i ryzyko, Komisja zbada, czy konieczne jest dalsze doprecyzowanie pojęcia szkodliwych treści audiowizualnych oraz jakie środki są niezbędne do zapewnienia, aby małoletni nie mieli kontaktu z takimi treściami.

Ponadto przyszły akt w sprawie sprawiedliwości cyfrowej ma na celu wzmocnienie i dostosowanie prawa ochrony konsumentów do zakładanych celów, również w środowisku cyfrowym, w pełnej zgodności z obowiązkami określonymi w niniejszym rozporządzeniu. Prawo ochrony konsumentów odgrywa ważną rolę w zapewnianiu, aby konsumenci, w tym dzieci, nie byli narażeni na nieuczciwe lub wprowadzające w błąd praktyki. W szczególności w dyrektywie o nieuczciwych praktykach handlowych uznano dzieci za konsumentów podatnych na zagrożenia, którzy wymagają zwiększonej ochrony; dyrektywa ta zabrania również bezpośredniego wzywania dzieci do nabycia reklamowanych produktów lub do nakłaniania rodziców lub innych osób dorosłych do kupienia im tych produktów. Dodatkowo w ramach przeglądu obowiązującego prawa ochrony konsumentów rozporządzenie w sprawie współpracy w dziedzinie ochrony konsumentów zostanie również zmienione w celu wzmocnienia istniejącego systemu koordynacji egzekwowania prawa dla organów krajowych i przyznania Komisji bezpośrednich uprawnień dochodzeniowych i egzekucyjnych w konkretnych przypadkach.

Ponadto niedawne zmiany w rozporządzeniu (UE) 2024/1689 zakazujące stosowania systemów AI generujących materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych, trwające przyjmowanie rozporządzenia w sprawie zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczania, wraz z niedawno przyjętą wersją przekształconą dyrektywy w sprawie niegodziwego traktowania dzieci w celach seksualnych, wzmacniają unijne ramy przeciwdziałania niegodziwemu traktowaniu dzieci w celach seksualnych i wykorzystywaniu seksualnemu dzieci, zarówno w internecie, jak i poza nim. Poprawią one zapobieganie, prowadzenie dochodzeń oraz udzielanie wsparcia ofiarom.

Wniosek jest również w pełni spójny i dodatkowo wspiera istniejące lub przyszłe inicjatywy mające na celu wzmocnienie pozycji i wspieranie małoletnich oraz zapewnienie im dobrostanu w internecie, w tym strategię UE na rzecz praw dziecka[8], zalecenie Komisji w sprawie rozwoju i wzmocnienia zintegrowanych systemów ochrony dzieci w najlepszym interesie dziecka[9], Plan działania w dziedzinie edukacji cyfrowej (2021–2027)[12], a także nadchodzący plan działania na rzecz przyszłości edukacji cyfrowej i umiejętności cyfrowych do 2030 r.

Bezpieczeństwo dzieci w internecie jest globalnym wyzwaniem wymagającym współpracy międzynarodowej. Wniosek jest spójny z polityką zewnętrzną Unii, w tym z międzynarodową strategią cyfrową (2025 r.), za pośrednictwem której UE rozszerza i pogłębia swoją współpracę dwustronną, regionalną i wielostronną. Wniosek harmonizuje przepisy w całej UE, co przyczyni się do zwiększenia skuteczności współpracy zewnętrznej UE i globalnego wpływu na bezpieczeństwo dzieci w internecie.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawę prawną niniejszego wniosku stanowi art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, który przewiduje ustanowienie środków mających na celu zapewnienie funkcjonowania rynku wewnętrznego. Niniejszy wniosek ma na celu zbliżenie przepisów w celu ustanowienia funkcjonowania rynku wewnętrznego oraz, zgodnie z art. 114 ust. 3, zapewnienie wysokiego poziomu ochrony zdrowia i bezpieczeństwa dzieci w całej Unii Europejskiej z uwzględnieniem nowych osiągnięć technologicznych.

Głównym celem niniejszego wniosku jest wprowadzenie zharmonizowanych przepisów mających na celu ochronę małoletnich w internecie. Ponieważ państwa członkowskie omawiają lub przyjmują nowe środki mające na celu ograniczenie dostępu do niektórych platform internetowych uznawanych za ryzykowne dla dzieci poniżej określonego wieku, istnieje ryzyko, że rynek UE stanie się coraz bardziej rozdrobniony. Niniejszy wniosek ma zatem na celu zapewnienie właściwego funkcjonowania rynku wewnętrznego, w szczególności w odniesieniu do dostarczania transgranicznych internetowych serwisów społecznościowych, usług platformy udostępniania wideo, sklepów z aplikacjami, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz gier internetowych. Takie zharmonizowane podejście zapewnia również jednakowo wysoki poziom ochrony małoletnich w całej UE.

Ponadto niniejszy wniosek doprecyzowuje i uzupełnia odpowiednie przepisy rozporządzenia (UE) 2022/2065 w zakresie ochrony małoletnich oraz uzupełnia rozporządzenie (UE) 2024/1689 w zakresie wymogów bezpieczeństwa dotyczących dzieci w odniesieniu do towarzyszy AI i ogólnych chatbotów konwersacyjnych. Ponieważ podstawę prawną zarówno rozporządzenia (UE) 2022/2065, jak i rozporządzenia (UE) 2024/1689 stanowi art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, w niniejszym wniosku przyjęto to samo podejście.

• Pomocniczość (w przypadku kompetencji niewyłącznych)

Biorąc pod uwagę, że usługi cyfrowe i systemy AI mają z założenia charakter transgraniczny, wspomniane powyżej działania ustawodawcze na szczeblu krajowym dotyczące odroczonego dostępu małoletnich utrudniają transgraniczne świadczenie usług i dostarczanie systemów cyfrowych oraz powodują niepewność prawa i przeszkody we wdrażaniu jednolitego rynku, wysokie koszty przestrzegania przepisów i nierówny poziom ochrony małoletnich w całej Europie.

Potencjalne konsekwencje braku natychmiastowych działań również wymagają pilnych rozwiązań. Państwa członkowskie przyjmują już własne przepisy w tym zakresie. W latach 2025 i 2026 otrzymano kilka powiadomień TRIS (Włochy, Francja, Norwegia, Grecja, Polska, Austria, Belgia) dotyczących ograniczeń wiekowych w odniesieniu do niektórych rodzajów usług cyfrowych. W prawie wszystkich pozostałych państwach członkowskich konsultacje są w toku, projekty są omawiane w parlamentach narodowych lub zostały ogłoszone przez rządy. Przepisy krajowe różnią się pod względem zakresu, limitów wiekowych i rodzajów nałożonych ograniczeń. Proponuje się w nich różne definicje lub kryteria rodzajów usług cyfrowych, do których dostęp ma być ograniczony, oraz różne limity wiekowe (od 13 do 16 lat), ostatecznie zależne od zgody rodziców. Niektóre z omawianych przepisów krajowych zawierają dodatkowe obowiązki w zakresie uwzględniania bezpieczeństwa na etapie projektowania. Mnożenie przepisów krajowych o różnych obowiązkach prawnych wiąże się ze znacznym ryzykiem fragmentacji jednolitego rynku, zmniejszenia pewności prawa i zwiększenia kosztów przestrzegania przepisów dla dostawców

usług cyfrowych, powodując przy tym nierówny poziom ochrony małoletnich w całej Unii Europejskiej.

Harmonizację przepisów mających na celu ochronę małoletnich i zapewnienie im bezpiecznego środowiska internetowego należy przeprowadzić na poziomie Unii, zapewniając w ten sposób przewidywalność i pewność, zmniejszając koszty przestrzegania przepisów w całej Europie i gwarantując, aby wszystkim małoletnim, niezależnie od miejsca zamieszkania, zapewniono wysoki poziom prywatności, bezpieczeństwa i ochrony w internecie.

- **Proporcjonalność**

Wniosek ma na celu zapewnienie solidnych i spójnych ram ochrony małoletnich w internecie. Wprowadza w tym celu ogólnounijne ograniczenie dostępu do mediów społecznościowych plus dla osób poniżej 13. roku życia. Podejście to umożliwia tworzenie kont rodzicielskich dla dzieci w wieku od 13 do 15 lat. Wniosek przewiduje zharmonizowany dostęp do bezpiecznych usług sieci społecznościowych i platform udostępniania wideo od 15. roku życia, w połączeniu z jasnymi obowiązkami w zakresie uwzględniania bezpieczeństwa na etapie projektowania oraz przejrzystymi wymogami i kryteriami dotyczącymi stosowania potwierdzania wieku.

We wniosku jako punkt wyjścia przyjęto sprawozdanie współprzewodniczących specjalnego panelu ds. bezpieczeństwa dzieci w internecie, w którym jasno określono zagrożenia, na jakie narażeni są małoletni w internecie. W tym kontekście wniosek wprowadza ramy, które pozwalają przeciwdziałać zagrożeniom dla usług wymienionych w sprawozdaniu, nie wywierając nieproporcjonalnego wpływu na prawa podstawowe (zob. sekcja poniżej).

Za sprawą kluczowych elementów niniejszego wniosku rozporządzenie ogranicza się do tego, co jest ściśle niezbędne do osiągnięcia celów wniosku. We wniosku określono w szczególności obowiązki dotyczące różnych rodzajów usług i systemów cyfrowych, w zależności od charakteru usługi lub systemu, aby zapewnić ich ukierunkowanie i proporcjonalność. Podejście to pomaga rozwiązać zidentyfikowane problemy, nie obciążając przy tym nadmiernie dostawców, których te problemy nie dotyczą. Istotne obowiązki ograniczają się do internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych oraz dostawców sklepów z aplikacjami. Zgodnie z podejściem współregulacyjnym opierają się one na inicjatywach współregulacyjnych dotyczących usług objętych zakresem niniejszego rozporządzenia, w tym w odniesieniu do sklepów z aplikacjami i gier internetowych. Jeżeli chodzi o systemy AI, wniosek ogranicza się do towarzyszy AI i ogólnych chatbotów konwersacyjnych, które mogą stwarzać poważne zagrożenia dla zdrowia, bezpieczeństwa i dobrostanu małoletnich i które nie są objęte wymogami uwzględniania bezpieczeństwa na etapie projektowania mającymi konkretnie na celu przeciwdziałanie tym zagrożeniom dla małoletnich na podstawie rozporządzenia (UE) 2024/1689.

Jednocześnie małe przedsiębiorstwa i mikroprzedsiębiorstwa nie są wyłączone z zakresu niniejszego rozporządzenia, ponieważ mogą również wyrządzać szkody małoletnim. Wyłączenie ich z zakresu stosowania byłoby sprzeczne z celem niniejszego wniosku.

Ze względu na małe prawdopodobieństwo wyrządzania szkody małoletnim wyłączone z zakresu stosowania są nienastawione na zysk encyklopedie internetowe, nienastawione na zysk repozytoria, usługi i systemy edukacyjne i naukowe, które zostały zaprojektowane wyłącznie do celów edukacyjnych i są obsługiwane w placówkach lub organizacjach

edukacyjnych, platformy tworzenia otwartego oprogramowania i platformy wymiany otwartego oprogramowania, chyba że sama platforma stanowi system AI objęty zakresem niniejszego rozporządzenia i rozporządzenia (UE) 2024/1689, usługi i systemy opracowane i obsługiwane wyłącznie do celów badań naukowych i rozwoju oraz usługi i systemy zaprojektowane, opracowane i obsługiwane przez organy publiczne i do wyłącznego użytku tych organów publicznych lub w ich imieniu.

Ustanawiając jasne ramy, którym towarzyszy współpraca między państwami członkowskimi, a także współregulacja, niniejszy wniosek ma na celu zwiększenie pewności prawa, zapewnienie funkcjonowania jednolitego rynku i osiągnięcie wyższego poziomu zaufania.

- **Wybór instrumentu**

Na podstawie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej prawodawca może przyjmować rozporządzenia i dyrektywy.

Komisja postanowiła przedstawić wniosek dotyczący rozporządzenia, aby zapewnić spójny poziom ochrony małoletnich w całej Unii oraz zapobiec rozbieżnościom utrudniającym swobodne świadczenie odpowiednich usług i korzystanie z odpowiednich systemów na rynku wewnętrznym. Jest to konieczne do zapewnienia pewności prawa i przejrzystości zarówno podmiotom gospodarczym, jak i dzieciom i ich rodzicom.

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

- **Konsultacje z zainteresowanymi stronami**

Wniosek jest bezpośrednio zgodny z zaleceniami współprzewodniczących specjalnego panelu ds. bezpieczeństwa dzieci w internecie. W ramach niezależnego procesu specjalny panel ds. bezpieczeństwa dzieci w internecie przeanalizował zagrożenia i możliwości dla dzieci w zakresie usług cyfrowych, a także istniejące ramy regulacyjne i występujące w nich luki. Zgromadził on obszerne dane i wiedzę fachową. W tym niezależnym procesie uczestniczyli eksperci z całej Unii Europejskiej z różnych dziedzin, w tym zdrowia, psychologii i psychiatrii dziecięcej, informatyki, technologii cyfrowej i mediów, nauk społecznych i praw dziecka. W spotkaniu wzięli również udział przedstawiciele grup młodzieżowych, grup rodziców i organizacji działających na rzecz praw dziecka. Dodatkowe zainteresowane strony, takie jak OHCHR, specjalistyczne ośrodki analityczne, przedstawiciele przemysłu, a także Europejska Rada Ochrony Danych, wniosły wkład w cały proces.

Podczas przygotowywania niniejszego wniosku przeprowadzono również konsultacje z młodzieżą. Młodzieżowa Rada Doradcza przy Przewodniczącej omówiła bezpieczeństwo i dobrostan dzieci w internecie na posiedzeniu w grudniu 2026 r., przedstawiając opinie dzieci ze wszystkich 27 państw członkowskich UE. W skład Rady wchodzi ponad 30 młodych przedstawicieli: po jednym przedstawicielu krajowej rady młodzieżowej każdego państwa członkowskiego UE, jeden przedstawiciel Europejskiego Forum Młodzieży oraz obserwatorzy z krajów kandydujących i potencjalnych krajów kandydujących do przystąpienia do UE. W grudniu 2025 r. na Forum na rzecz Bezpieczniejszego Internetu, w którym uczestniczyło ponad 200 dzieci, młodych osób oraz przedstawicieli społeczeństwa obywatelskiego, przemysłu i organów krajowych, omówiono temat „Dlaczego wiek ma znaczenie: ochrona i wzmocnienie pozycji młodzieży w erze cyfrowej”. Ambasadorzy młodzieżowi inicjatywy „Lepszy internet dla dzieci” i przedstawiciele młodzieży z platform uczestnictwa dzieci mieli również czynny udział w specjalnym panelu. We wszystkich

grupach przedstawiciele młodzieży podkreślili odpowiedzialność dostawców usług cyfrowych za świadczenie bezpiecznych i dostosowanych do wieku usług. Uwypuklili również potrzebę wprowadzenia wymogów uwzględniania bezpieczeństwa na etapie projektowania, w tym dostosowanych do wieku ustawień domyślnych, systemów rekomendacji i projektowania interfejsów.

Uzupełnieniem tego procesu konsultacyjnego jest szersze zaangażowanie zainteresowanych stron Komisji w obszarze bezpieczeństwa dzieci w internecie. Obejmuje to procesy konsultacyjne realizowane w kontekście wdrażania i egzekwowania aktu o usługach cyfrowych, a także strategii na rzecz lepszego internetu dla dzieci i jej sieci centrów bezpieczniejszego internetu oraz ambasadorów młodzieżowych inicjatywy „Lepszy internet dla dzieci". W kontekście przyjęcia wytycznych dotyczących ochrony małoletnich na podstawie rozporządzenia (UE) 2022/2065 zaproszenie do zgłaszania uwag z 2024 r., w ramach którego otrzymano ponad 170 informacji zwrotnych, oraz konsultacje publiczne z 2025 r., w ramach których otrzymano ponad 300 uwag, dostarczyły szczegółowych informacji od szerokiego grona zainteresowanych stron, w tym badaczy, społeczeństwa obywatelskiego, przemysłu i organów publicznych, na temat dobrych praktyk i środków dotyczących platform internetowych w celu zaprojektowania bezpiecznej usługi online dla dzieci. Większość respondentów wyraziła pozytywną opinię na temat środków wprowadzonych w wytycznych, które w dużej mierze skodyfikowano w niniejszym wniosku. Respondenci zwrócili się również o doprecyzowanie charakteru prawnego wytycznych oraz sytuacji, w których weryfikacja wieku i szacowanie wieku są właściwe.

W okresie od marca do kwietnia 2026 r. Komisja przeprowadziła badanie Eurobarometr na temat wpływu nadmiernego czasu spędzanego przed ekranem oraz mediów społecznościowych na zdrowie psychiczne młodych ludzi, gromadząc dane od ponad 26 000 osób w wieku 13–18 lat i ponad 12 000 rodziców we wszystkich 27 państwach członkowskich. Z ustaleń wynika, że czas spędzany przed ekranem stanowi przeważającą część codziennego życia nastolatków, co niesie ze sobą poważne zagrożenia, ponieważ dziewięcioro na dziesięcioro nastolatków napotkało co najmniej raz w ciągu ostatnich trzech miesięcy szkodliwe lub niepokojące treści w internecie, przy czym obawy dotyczą również szkód interpersonalnych i cyberszykanowania. 54 % rodziców i 45 % osób w wieku 13–18 lat uważa opóźnienie dostępu ze względu na wiek za skuteczne rozwiązanie, a 47 % rodziców i 48 % nastolatków wzywa do skuteczniejszego wdrażania obowiązujących przepisów przez usługi cyfrowe.

Ponadto Komisja otrzymuje na bieżąco dodatkowe źródła dowodów od Europejskiej Rady ds. Usług Cyfrowych i krajowych koordynatorów ds. usług cyfrowych, którzy są odpowiedzialni za nadzór nad mniejszymi platformami internetowymi i zapewnienie im bezpiecznego środowiska dla małoletnich oraz którzy ściśle monitorują ten obszar w terenie.

Dodatkowe procesy konsultacyjne prowadzono również w ramach powiązanych inicjatyw europejskich, takich jak akt w sprawie sprawiedliwości cyfrowej i dyrektywa o audiowizualnych usługach medialnych. Konsultacje i zaproszenie do zgłaszania uwag dotyczące aktu w sprawie sprawiedliwości cyfrowej otwarto na 12 tygodni w dniu 17 lipca 2025 r. Zebrano w nich obszerne informacje zwrotne od obywateli, organów publicznych i innych zainteresowanych stron, gromadząc istotne dowody dotyczące uzależniających cech projektowych produktów cyfrowych oraz zwodniczego lub manipulacyjnego projektowania interfejsów, w tym wpływu takich praktyk na małoletnich. Na przykład w ramach strategii UE na rzecz praw dziecka przeprowadzono konsultacje na temat sprawiedliwości cyfrowej z udziałem 5 000 dzieci z unijnej platformy uczestnictwa dzieci. Ponadto 10 lutego 2026 r.

Komisja rozpoczęła konsultacje publiczne na potrzeby oceny skutków dyrektywy o audiowizualnych usługach medialnych, gromadząc informacje zwrotne od równie szerokiego grona zainteresowanych stron, w tym na temat najlepszych sposobów wzmocnienia ochrony małoletnich w internecie. Oba procesy konsultacyjne dostarczyły istotnych dowodów do celów niniejszego wniosku.

- **Ocena skutków**

Najważniejsze elementy niniejszego wniosku opierają się na obszernym zbiorze dowodów pochodzących z bardzo różnych źródeł, w tym na ocenach skutków stanowiących podstawę innych już przyjętych lub przyszłych inicjatyw ustawodawczych.

W związku z tym proponowane rozporządzenie i towarzyszący mu dokument roboczy służb Komisji dotyczący skutków wniosku opierają się na solidnej bazie dowodowej.

Po pierwsze, specjalny panel ds. bezpieczeństwa dzieci w internecie zgromadził ponad 60 ekspertów z różnych dziedzin, w tym w dziedzinie zdrowia, psychologii i psychiatrii dziecięcej, informatyki i nauk społecznych, a także przedstawicieli grup młodzieżowych, grup rodziców i organizacji działających na rzecz praw dziecka, a współprzewodniczący spotkali się również z OHCHR, specjalistycznymi ośrodkami analitycznymi, przedstawicielami przemysłu i Europejską Radą Ochrony Danych.

Po drugie, specjalna analiza skutków przedstawiona w dokumencie roboczym służb Komisji opiera się na istniejących ocenach skutków, w tym w odniesieniu do aktu o usługach cyfrowych, aktu o rynkach cyfrowych, aktu w sprawie sztucznej inteligencji, wniosku dotyczącego rozporządzenia w sprawie zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczania oraz przekształconej dyrektywy w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych, a także przyszłego aktu w sprawie sprawiedliwości cyfrowej i dyrektywy o audiowizualnych usługach medialnych.

Po trzecie, dowody i dane gromadzi się w drodze wdrażania i egzekwowania aktu o usługach cyfrowych, w szczególności 10 wstępnych ustaleń w odniesieniu do ochrony małoletnich, w tym dotyczących uzależniających cech projektowych, bezpiecznych kont i potwierdzania wieku, a także badań, sprawozdań z oceny ryzyka i zaangażowania zainteresowanych stron, w szczególności podczas opracowywania wytycznych dotyczących ochrony małoletnich, które obejmowały zaproszenie do zgłaszania uwag, konsultacje publiczne, współpracę z dziećmi i młodzieżą oraz spotkania z Europejską Radą ds. Usług Cyfrowych. W tym kontekście trwa współpraca z organami krajowymi w ramach nadzoru i egzekwowania aktu o usługach cyfrowych. Stanowi to cenny wkład w dochodzenia, a wiele państw członkowskich, takich jak Szwecja i Niemcy, przeprowadziło dochodzenia i konsultacje dotyczące krajowych projektów ustaw o ochronie małoletnich.

Po czwarte, międzynarodowe zaangażowanie i współpraca wskazują ponadto na źródła dowodów pochodzących od organów publicznych i organów regulacyjnych. Komisja ściśle współpracuje z innymi organami regulacyjnymi, w tym z Australią i Zjednoczonym Królestwem, które przeprowadziły badania i oceny skutków, a także z Brazylią i Japonią.

Po piąte, dodatkowe badania obejmują szeroki zakres badań akademickich, badanie Eurobarometr na temat wpływu nadmiernego czasu spędzanego przed ekranem i mediów społecznościowych na zdrowie psychiczne młodych ludzi przeprowadzone w 2026 r. oraz

badanie zlecone przez Komisję na temat wpływu potwierdzania wieku na prawa podstawowe i jego koszty gospodarcze.

Komisja przygotowała towarzyszący dokument roboczy służb Komisji zawierający (i) definicję problemu, (ii) wyjaśnienie zastosowanego podejścia oraz (iii) ocenę skutków. Dokument roboczy służb Komisji opiera się na sprawozdaniu współprzewodniczących specjalnego panelu, a także na dowodach i danych zgromadzonych w kontekście wdrażania i egzekwowania aktu o usługach cyfrowych oraz przygotowywania ocen skutków, w szczególności w odniesieniu do aktu w sprawie sprawiedliwości cyfrowej i przeglądu dyrektywy o audiowizualnych usługach medialnych.

W dokumencie roboczym służb Komisji przedstawiono główne skutki społeczne i gospodarcze wniosku. Jeżeli chodzi o skutki społeczne, jako bezpośredni i pośredni wpływ wniosku należy poprawić dobrostan małoletnich. Dzięki opóźnieniu dostępu do niektórych konkretnych usług i zapewnieniu zabezpieczeń dla usług cyfrowych dostosowanych do wieku środowisko internetowe stanie się bezpieczniejszym miejscem dla małoletnich, ograniczając ryzyko, jakie napotykają w internecie, a także jego wpływ na ich rozwój poznawczy, zdrowie fizyczne i psychiczne.

Jeżeli chodzi o skutki gospodarcze, oczekuje się, że koszty krańcowe wprowadzone niniejszym wnioskiem pozostaną stosunkowo ograniczone w odniesieniu do wdrożenia większości wymogów uwzględniania bezpieczeństwa na etapie projektowania, ponieważ wymogi te były już zawarte w wytycznych w sprawie ochrony małoletnich na podstawie art. 28 aktu o usługach cyfrowych. Wymogi dotyczące przygotowywania planów zapewniania zgodności i polegania na audytach zostały już w dużej mierze uwzględnione w ocenach ryzyka i przepisach dotyczących audytu zawartych w akcie o usługach cyfrowych. Dotyczą one również dostawców o bardzo dużej bazie użytkowników (45 mln aktywnych użytkowników miesięcznie), co powinno ograniczyć wpływ na MŚP, które co do zasady nie osiągają skali bazy użytkowników równoważnej skali bardzo dużych platform internetowych. Wdrożenie środków potwierdzania wieku i narzędzi kontroli rodzicielskiej spowoduje dodatkowe koszty dla dostawców usług cyfrowych. Nie jest możliwe jednoznaczne określenie kosztów tych dostosowań i ich częstotliwości, zwłaszcza w przypadku potencjalnie dużej liczby małych dostawców i mikrodostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo i gier wideo, którzy wcześniej nie podlegali art. 28 aktu o usługach cyfrowych. Koszty te są jednak łagodzone dzięki opracowaniu unijnego rozwiązania z zakresu weryfikacji wieku, oczekiwanemu zwiększonemu rozwojowi rynku bezpiecznych rozwiązań projektowych oraz faktowi, że podobne wymogi istnieją już w prawie UE i w coraz większym stopniu w państwach trzecich. Należy również wziąć pod uwagę, że wielu dostawców usług cyfrowych prawdopodobnie ponosiłoby wiele z tych kosztów wielokrotnie na mocy przepisów krajowych, dlatego przyjęcie zharmonizowanych przepisów byłoby dla nich korzystne.

- **Prawa podstawowe**

Wniosek ma na celu poprawę, promowanie i wspieranie poszanowania praw dziecka w internecie, zapisanych w Karcie praw podstawowych Unii Europejskiej („Karta”). Celem odroczenia dostępu jest zapewnienie przestrzegania kompleksowych praw dziecka w internecie, w tym prawa do ochrony niezbędnej dla dobrostanu dziecka, jego zdrowia i bezpieczeństwa, prywatności, uczestnictwa, swobodnego wyrażania poglądów, stosownie do jego wieku i dojrzałości, z uwzględnieniem przede wszystkim jego najlepszego interesu, przy zapewnieniu mu prawa do rozwoju i samostanowienia wolnego od ryzyka i szkód stwarzanych przez niektóre usługi i systemy internetowe. Chociaż usługi objęte zakresem

niniejszego rozporządzenia stwarzają znaczne ryzyko dla zdrowia i bezpieczeństwa dzieci, umożliwiają one również dzieciom swobodne wyrażanie poglądów oraz otrzymywanie i przekazywanie pomysłów, zgodnie z ochroną na mocy art. 24 ust. 1 i art. 11 ust. 1 Karty. W związku z tym odroczenie dostępu jest ściśle ograniczone do tworzenia kont w wyraźnie zdefiniowanym zestawie usług i systemów cyfrowych, które wykorzystują określone cechy projektowe i udostępniają małoletnim określone funkcje, co do których udowodniono, że są szkodliwe dla zdrowia i bezpieczeństwa małoletnich. Środek ten zapewnia, aby to ograniczenie prawa dziecka do wolności wypowiedzi pozostało proporcjonalne i konieczne do osiągnięcia celu interesu ogólnego zgodnie z wymogami Karty. Nie należy ograniczać dostępu do usług, które są bezpieczne, dostosowane do wieku, przeznaczone dla dzieci i umożliwiają odpowiednią kontrolę rodzicielską i nadzór. Ponadto przewidziano wyjątki od opóźnienia dostępu, aby zapewnić dostęp do informacji, materiałów edukacyjnych i usług publicznych.

Zgodnie z uwagą ogólną nr 25 Komitetu Praw Dziecka ONZ ustanowiono wymogi uwzględniania bezpieczeństwa na etapie projektowania w celu zapewnienia poszanowania praw dziecka w internecie. Bezpieczne ustawienia zapewnią dzieciom dodatkową prywatność, a ograniczone kontakty z nieznajomymi zmniejszą ryzyko cyberszykanowania i nagabywania dzieci dla celów seksualnych.

Rodzice i opiekunowie również odgrywają ważną rolę w wychowaniu i rozwoju swoich dzieci, co uznano w art. 24 ust. 3 Karty praw podstawowych Unii Europejskiej. Poszanowanie życia prywatnego i rodzinnego, domu i komunikowania się jest zagwarantowane w art. 7 Karty. Art. 14 ust. 3 Karty zapewnia poszanowanie wolności tworzenia placówek edukacyjnych z należytym poszanowaniem zasad demokratycznych oraz prawa rodziców do zapewnienia wychowania i nauczania dzieci zgodnie z ich przekonaniami religijnymi, filozoficznymi i pedagogicznymi, zgodnie z przepisami krajowymi regulującymi korzystanie z tej wolności i tego prawa, przy jednoczesnym zapewnieniu poszanowania innych praw podstawowych zapisanych w Karcie, w tym art. 21 dotyczącego niedyskryminacji i art. 24 dotyczącego praw dziecka, z uwzględnieniem przede wszystkim ich najlepszego interesu.

Uznając tę ważną rolę rodziców i opiekunów, we wniosku przewidziano narzędzia dla opiekunów i umożliwiono rodzicom zakładanie kont w bezpiecznym środowisku dla małoletnich w wieku 13–15 lat. Narzędzia te muszą być udostępniane zgodnie ze zmieniającymi się zdolnościami dzieci i z poszanowaniem ich prawa do prywatności.

Niniejsze rozporządzenie zapewnia również poszanowanie praw dzieci poprzez wzmocnienie ich autonomii. Rozporządzenie nakłada na dostawców usług i systemów cyfrowych objętych jego zakresem obowiązek zapewnienia łatwo dostępnych i przyjaznych dziecku systemów zgłaszania. Dostawcy ci muszą dopilnować, aby zgłoszenia małoletnich i opiekunów były traktowane priorytetowo. Rozporządzenie umożliwia również dalszą kontrolę nad ustawieniami małoletnich. Ponadto wniosek pomaga dzieciom w edukacji cyfrowej, rozwijaniu umiejętności czytania i pisania oraz wsparciu ze strony rodziców, opiekunów, nauczycieli i wychowawców, ponieważ przewiduje, że państwa członkowskie opracują krajowe strategie wspierające cele ochrony dzieci w internecie.

Systemy potwierdzania wieku i wymóg weryfikacji wieku użytkowników mogą potencjalnie mieć istotny wpływ na prawo do prywatności, a także na wolność wypowiedzi, uczestnictwo i niedyskryminację użytkowników. We wniosku określono jasne wymogi dotyczące wdrażania i stosowania systemów potwierdzania wieku, a także zabezpieczenia i środki przejściowe mające na celu ograniczenie wpływu na te prawa podstawowe do tego, co jest absolutnie niezbędne do ochrony zdrowia i bezpieczeństwa małoletnich w internecie. Kryteria te obejmują wysoki poziom dokładności, wiarygodności, odporności, bezpieczeństwa,

niedyskryminacji i nieinwazyjności. Zgodnie z podejściem opartym na analizie ryzyka i przy zapewnieniu proporcjonalności weryfikacja wieku jest wymagana wyłącznie w celu wdrożenia odroczenia dostępu i ogranicza się do nowych kont i istniejących kont tylko wtedy, gdy dostawca nie jest w stanie z wysokim stopniem pewności stwierdzić, że posiadacz konta osiągnął wymagany wiek. Poprzez zapisanie tych kryteriów w prawie we wniosku przewidziano jasne normy prawne dotyczące stosowania i wdrażania systemów potwierdzania wieku zapewniających wysoki standard ochrony danych w odniesieniu do ich stosowania. Będzie to sprzyjać wdrażaniu innowacyjnego rynku rozwiązań w zakresie potwierdzania wieku na jednolitym rynku cyfrowym z poszanowaniem praw podstawowych.

4. WPŁYW NA BUDŻET

Ważne jest, aby Komisja dysponowała wystarczającą liczbą pracowników do prowadzenia działań na podstawie niniejszego rozporządzenia. Jest to szczególnie istotne, ponieważ wykonując swoje zadania, Komisja będzie musiała nadzorować niektóre z najsilniejszych finansowo i najbardziej zaawansowanych technologicznie przedsiębiorstw na świecie. Nadzór nad tymi przedsiębiorstwami będzie wymagał pracowników o wysokich kwalifikacjach i specjalistycznych profilach. Komisja jest narażona na wysokie ryzyko polityczne w przypadku niedostatecznych zasobów na egzekwowanie przepisów. Coraz częściej wzywa się do podjęcia pilnych działań w celu ochrony europejskich dzieci w internecie, a zapewnienie skutecznej ochrony następnego pokolenia wymaga odpowiedniego personelu – również w celu zapewnienia przyspieszonego egzekwowania przepisów, które będzie wymagane na mocy niniejszego rozporządzenia.

W tym celu Komisja będzie opierać się na opłacie nadzorczej ustanowionej w art. 43 aktu o usługach cyfrowych. Ponieważ niniejszy wniosek stanowi doprecyzowanie aktu o usługach cyfrowych, przeznaczone na niego zasoby powinny również opierać się na tej samej opłacie nadzorczej. Dalsze szczegółowe informacje na temat wpływu na budżet przedstawiono w ocenie skutków finansowych i cyfrowych regulacji.

5. ELEMENTY FAKULTATYWNE

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

Wniosek zostanie poddany rygorystycznej ocenie, w szczególności pod względem skuteczności odroczenia dostępu, zakresu podmiotowego odroczenia dostępu i jego proporcjonalności oraz wymogów uwzględniania bezpieczeństwa na etapie projektowania. Ocena ta będzie uwzględniać doświadczenie zdobyte podczas wdrażania wniosku, a także zmiany technologiczne, rynkowe i prawne.

Uzupełni to bieżące monitorowanie na podstawie aktu o usługach cyfrowych.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

W **rozdziale I** ustanowiono przepisy ogólne, w tym dotyczące przedmiotu i zakresu stosowania rozporządzenia (art. 1 i art. 2) oraz definicje najważniejszych pojęć stosowanych w rozporządzeniu (art. 3). W sekcjach tych określono również zasady przeciwdziałające obchodzeniu przepisów w odniesieniu do dostawców objętych zakresem niniejszego rozporządzenia (art. 4) oraz obowiązki zidentyfikowanych dostawców dotyczące powiadamiania o niezależnym audycie planu zapewnienia zgodności i poddania się mu (art. 5).

Rozdział II zawiera przepisy dotyczące odroczonego dostępu małoletnich do mediów społecznościowych, określające, że dostawcy usług, które mają szczególne cechy i które stanowią usługi sieci społecznościowych lub usługi platform udostępniania wideo, lub obie te usługi, nie powinni zezwalać małoletnim w wieku poniżej 15 lat na założenie niezależnego konta. Ponadto dostawcy tych usług mogą zezwolić opiekunom na zakładanie kont dla małoletnich w wieku powyżej 13 lat z ograniczonymi cechami dostosowanymi do wieku, aby uzyskać dostęp do usługi (art. 6). W przypadku gdy dostawcy usług platformy udostępniania wideo mogą wykazać, że usługa ta jest dostosowana do wieku, mogą oni wyjątkowo zezwolić opiekunom na umożliwienie dostępu również małoletnim poniżej 13. roku życia za pośrednictwem kont utworzonych i nadzorowanych przez samych opiekunów (art. 7).

W **rozdziale III** określono przepisy dotyczące uwzględniania bezpieczeństwa na etapie projektowania mające zastosowanie do dostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo, towarzyszy AI, ogólnych chatbotów konwersacyjnych i gier internetowych.

W **sekcji 1** określono przepisy ogólne mające zastosowanie do dostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo, towarzyszy AI, ogólnych chatbotów konwersacyjnych, gier internetowych oraz sklepów z aplikacjami. W sekcji tej wskazano, że wymogi określone w niniejszym rozdziale mają również zastosowanie do niezarejestrowanych odbiorców usługi lub użytkowników systemu oraz że odstępstwo od tych wymogów jest możliwe tylko wtedy, gdy ustalono, że odbiorca usługi lub użytkownik systemu jest osobą dorosłą, z wykorzystaniem potwierdzania wieku zgodnie z rozdziałem V (art. 8).

W **sekcji 2** określono przepisy mające zastosowanie do internetowych serwisów społecznościowych i usług platformy udostępniania wideo. W szczególności usługom tym zabrania się projektowania, organizowania lub świadczenia usług w sposób, który ma na celu zachęcać (lub w przypadku którego można racjonalnie przewidzieć, że będzie zachęcać) małoletnich do kompulsywnego lub nadmiernego korzystania z usługi oraz należy wprowadzić skuteczne narzędzia zarządzania czasem, które chronią najważniejsze godziny snu i czas szkolny małoletnich (art. 9). Dostawcy, którzy korzystają z systemów rekomendacji, są zobowiązani do projektowania sugerowanych informacji i optymalizowania swoich systemów rekomendacji dla małoletnich w sposób zapewniający wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich (art. 10). Ponadto dostawcy ci mają obowiązek wprowadzić odpowiednie i proporcjonalne środki w celu zapewnienia, aby ustawienia obejmowały domyślnie wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, który nie może zostać zmieniony, chyba że małoletni wyraźnie zgodzili się na takie zmiany. Dostawcy ci mają obowiązek zapewnić, aby funkcje lub ustawienia, które mają jakikolwiek rzeczywisty lub przewidywalny negatywny wpływ na prywatność, bezpieczeństwo i ochronę małoletnich, nie były dla nich dostępne (art. 11). Te internetowe serwisy społecznościowe i usługi platformy udostępniania wideo są również zobowiązane do wprowadzenia środków zapewniających wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w odniesieniu do kontaktów między małoletnimi a innymi odbiorcami usługi (art. 12). Ponadto ci sami dostawcy mają obowiązek zapewnić, aby przed dokonaniem transakcji gospodarczej małoletni mieli jasność co do tego, że jest to transakcja gospodarcza, oraz aby ich wciąż rozwijająca się wiedza w dziedzinie handlu nie była wykorzystywana poprzez wybory projektowe, organizacyjne lub operacyjne, które mogą prowadzić do nadmiernych, impulsywnych lub niepożądanych wydatków, co obejmuje nienarażanie małoletnich na systemy zmiennych nagród (art. 13).

W **sekcji 3** określono przepisy mające zastosowanie do towarzyszy AI i ogólnych chatbotów konwersacyjnych. W szczególności sekcja ta zobowiązuje dostawców do wdrożenia przepisów dotyczących uwzględniania bezpieczeństwa na etapie projektowania w odniesieniu do uzależniających cech projektowych, bezpiecznych ustawień i przejrzystości transakcji handlowych określonych w art. 9, 11 i 13 sekcji 2, a także szczegółowych przepisów dostosowanych do tych systemów (art. 14). Przepisy te nakładają na dostawców towarzyszy AI i ogólnych chatbotów konwersacyjnych obowiązek wprowadzenia silnej ochrony bezpieczeństwa dzieci, w tym zaprojektowania systemów w taki sposób, aby małoletni nie byli narażeni na funkcje, które mogą powodować zależności emocjonalne, a także zapobiegania szkodliwym interakcjom oraz przeprowadzania testów i monitorowania po wprowadzeniu do obrotu w celu identyfikacji i łagodzenia szkód dla bezpieczeństwa, zdrowia, praw podstawowych oraz dobrostanu i rozwoju małoletnich. W przypadku gdy takie systemy są wdrażane jako funkcja internetowych serwisów społecznościowych, usług platformy udostępniania wideo lub gier internetowych, dostawcy tych usług powinni zapewnić, aby towarzysze AI i ogólne chatboty konwersacyjne nie były automatycznie aktywowane i aby małoletni mieli możliwość rezygnacji z korzystania z nich, jeżeli jest to możliwe, i nie byli zachęcani do takiego korzystania.

Sekcja 4 zawiera przepisy mające zastosowanie do gier internetowych. W szczególności sekcja ta zobowiązuje dostawców do wdrożenia przepisów dotyczących uwzględniania bezpieczeństwa na etapie projektowania w odniesieniu do uzależniających cech projektowych i bezpiecznych ustawień określonych w art. 9, 11 i 12 sekcji 2, a także szczegółowych przepisów dostosowanych do gier internetowych (art. 15). Przepisy te przewidują między innymi, że dostawcy gier internetowych będą mieli obowiązek wdrożyć zabezpieczenia zapobiegające wykorzystywaniu gier internetowych do nakłaniania małoletnich do nawiązywania kontaktów w ramach innych usług, które mogą stanowić zagrożenie dla ich prywatności, bezpieczeństwa i ochrony. W przypadku gdy dostawcy platform gier wideo zezwalają odbiorcom na tworzenie gier wideo, dostawca ma obowiązek zastosować niezbędne oprogramowanie i organizację, aby umożliwić tym grom wideo wywiązanie się z obowiązków określonych w art. 15 ust. 1 i 2 oraz art. 18 i 20.

W **sekcji 5** określono przepisy dotyczące dostępu dostosowanego do wieku mające zastosowanie do dostawców sklepów z aplikacjami. W sekcji tej zobowiązuje się tych dostawców do wprowadzenia systemu klasyfikacji wiekowej w celu ustalenia, czy aplikacje są dostosowane do wieku, oraz do oceny wieku usługobiorcy poprzez potwierdzanie wieku. W przypadku gdy danej aplikacji nie uznaje się za odpowiednią do wieku, dostawca sklepu z aplikacjami nie może zezwalać małoletnim na dostęp do takich aplikacji, które nie są odpowiednie do ich wieku (art. 16). Ponadto w sekcji tej zachęca się do opracowania kodeksów postępowania, które przyczynią się do zharmonizowanego ustanowienia i stosowania systemów klasyfikacji wiekowej (art. 17).

W **sekcji 6** określono dodatkowe ogólne obowiązki dotyczące sprawczości małoletnich, a także narzędzia wzmacniające pozycję małoletnich i opiekunów mające zastosowanie do dostawców usług sieci społecznościowych, usług platform udostępniania wideo, towarzyszy AI, ogólnych chatbotów konwersacyjnych oraz platform gier wideo i gier. W sekcji tej określono, że dostawcy ci są zobowiązani do zapewnienia, aby funkcje, komunikacja, informacje, narzędzia i mechanizmy kontroli użytkownika usługi, ostrzeżenia i wszelkie inne informacje, o których mowa w rozdziale III, były łatwo dostępne dla wszystkich małoletnich i przedstawione w sposób dla nich zrozumiały. Dostawcy bardzo dużych platform internetowych w rozumieniu art. 33 ust. 1 rozporządzenia (UE) 2022/2065 są zobowiązani do przedstawiania takich informacji w języku urzędowym lub językach urzędowych państwa

członkowskiego lub państw członkowskich, w których świadczona jest usługa. Ponadto dostawcy usług sieci społecznościowych, usług platform udostępniania wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz platform gier wideo są zobowiązani do zapewnienia narzędzi umożliwiających małoletnim kontrolowanie treści i ustawień oraz przekazywanie informacji zwrotnych, które powinny mieć trwały wpływ na zalecane treści (art. 18). W sekcji tej określono również, że dostawcy ci są zobowiązani do wprowadzenia przyjaznych dziecku mechanizmów zgłaszania i narzędzi wsparcia dla małoletnich (art. 19), a także skutecznych i łatwych w użyciu narzędzi dla opiekunów. Ponadto w sekcji tej zobowiązano tych dostawców usług sieci społecznościowych, usług platform udostępniania wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz gier internetowych do zachęcania do wprowadzania takich narzędzi oraz zobowiązano dostawców bardzo dużych platform internetowych w rozumieniu art. 33 ust. 1 rozporządzenia (UE) 2022/2065 do zapewnienia interoperacyjności tych narzędzi dla opiekunów z narzędziami dla opiekunów zapewnianymi przez osoby trzecie, zgodnie z warunkami określonymi w art. 6 rozporządzenia (UE) 2022/1925 (art. 20). Ponadto w sekcji tej określono, że małoletni i opiekunowie mają prawo wnieść skargę do właściwego organu przeciwko dostawcom usług sieci społecznościowych, usług platform udostępniania wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz gier internetowych, w przypadku których zarzuca się naruszenie niniejszego rozporządzenia, oraz że małoletni i opiekunowie mają prawo upoważnić organ, organizację lub stowarzyszenie do wykonywania praw przyznanych niniejszym rozporządzeniem w imieniu małoletniego lub jego opiekuna (art. 21).

Sekcja 7 zawiera inne przepisy dotyczące należytej staranności na rzecz bezpiecznego środowiska internetowego. Określono w niej obowiązki bardzo dużych platform internetowych w zakresie monitorowania (art. 22), przepisy dotyczące sporządzania kodeksów postępowania (art. 23) oraz obowiązek posiadania przez usługi przedstawicieli prawnych (art. 24). Ponadto w sekcji tej określono, że Komisja jest uprawniona do przyjmowania aktów delegowanych w celu uzupełnienia środków wymienionych w tym rozdziale, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich korzystających z tych usług (art. 25).

Rozdział IV określa obowiązek weryfikacji odpowiedzialności rodzicielskiej (art. 26).

Rozdział V zawiera przepisy dotyczące potwierdzania wieku.

W **sekcji 1** zdefiniowano ogólne zasady potwierdzania wieku. W sekcji tej określono, że w przypadku gdy dostawcy objęci zakresem rozdziałów II i III muszą wdrożyć rozwiązania w zakresie potwierdzania wieku, mają oni obowiązek zapewnić wysoki poziom dokładności, wiarygodności, odporności, nieinwazyjności, prywatności i niedyskryminacji, a oświadczenie własne nie jest wystarczające do zapewnienia zgodności z niniejszym rozporządzeniem (art. 27). Sekcja ta zawiera również szczegółowe przepisy dotyczące ochrony danych w ramach potwierdzania wieku (art. 28).

Sekcja 2 uzupełnia powyższe zasady o szczególne obowiązki w zakresie potwierdzania wieku, stanowiąc, że do celów zgodności z art. 5 i 6 dostawcy powinni wprowadzić weryfikację wieku, a do celów zgodności z rozdziałem III mogą stosować zarówno weryfikację wieku, jak i inne rozwiązania w zakresie potwierdzania wieku na określonych warunkach (art. 29), uzupełnione uprawnieniem Komisji do określenia szczegółów zdefiniowanych w rozdziale dotyczącym potwierdzania wieku (art. 30). Ponadto w sekcji tej zobowiązano państwa członkowskie do wdrożenia niezbędnych środków w celu zapewnienia dostępności różnych sposobów uzyskania poświadczenia dowodu wieku na potrzeby

weryfikacji minimalnego wieku oraz do udostępnienia co najmniej jednego rozwiązania z zakresu weryfikacji wieku (art. 31). W sekcji tej określono również środki dotyczące weryfikacji wieku w odniesieniu do istniejących kont (art. 32).

Rozdział VI wprowadza przepis dotyczący środków wdrażanych przez państwa członkowskie w celu przygotowania i wspierania małoletnich w miarę wprowadzania w życie niniejszego rozporządzenia (art. 33).

Rozdział VII zawiera przepisy dotyczące kompetencji, nadzoru i egzekwowania przepisów niniejszego wniosku, które opierają się na istniejących strukturach i ramach egzekwowania przepisów na podstawie rozporządzenia (UE) 2022/2065 i rozporządzenia (UE) 2024/1689, aby uniknąć powielania działań i zapewnić spójność z obowiązującymi przepisami dotyczącymi usług pośrednich i systemów AI (art. 34). W przypadku gdy Komisja wszczyna postępowanie w odniesieniu do usług i systemów wchodzących w zakres jej wyłącznych kompetencji, dąży ona do przyjęcia ostatecznej decyzji w terminie 90 dni i przekazuje wstępne ustalenia zainteresowanemu dostawcy usług w terminie 30 dni od wszczęcia postępowania (art. 35). Ponadto rozdział ten zawiera przepis dotyczący finansowania przez Komisję działań w zakresie nadzoru i egzekwowania przepisów na podstawie niniejszego rozporządzenia (art. 36) oraz przepisy dotyczące rozwoju wiedzy fachowej i mechanizmów reagowania na incydenty (art. 37 i 38).

Rozdział VIII określa przepisy dotyczące aktów wykonawczych i delegowanych (art. 39 i 40), zaś **rozdział IX** zawiera przepisy końcowe, w tym przepisy dotyczące przeglądu rozporządzenia, włączenia niniejszego rozporządzenia do załącznika do dyrektywy w sprawie powództw przedstawicielskich (art. 41) oraz wejścia w życie i stosowania (art. 42 i 43).

2026/0286 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

EU KIDS ACT – „UE na straży odpowiedzialnych i godnych zaufania przestrzeni cyfrowych w internecie”

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],

uwzględniając opinię Komitetu Regionów[2],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Internetowe serwisy społecznościowe, usługi platformy udostępniania wideo, towarzysze AI (sztucznej inteligencji), ogólne chatboty konwersacyjne, gry internetowe i sklepy z aplikacjami stały się ważną częścią codziennego życia małoletnich. Takie usługi społeczeństwa informacyjnego i systemy AI stwarzają dla małoletnich możliwości w zakresie rozwoju tożsamości, uczenia się, edukacji, zaangażowania obywatelskiego, budowania relacji, komunikacji, nawiązywania kontaktów oraz kreatywności. Jednocześnie niektóre z tych usług i systemów, także ze względu na ich konstrukcję, mogą stwarzać zagrożenie dla prywatności, bezpieczeństwa i ochrony małoletnich. Zagrożenie to obejmuje na przykład narażenie na treści nielegalne czy też treści oraz ryzyko wynikające z cyberszykanowania lub kontaktu z osobami działającymi na szkodę małoletnich. Małoletni – jako konsumenci podatni na zagrożenia – mogą być również narażeni na ryzyko ze względu na praktyki handlowe, które mogą być manipulacyjne i powodować niepożądane wydatki oraz kompulsywne i uzależniające zachowania. Ryzyko to może wynikać z bezpośredniego doświadczenia małoletniego z internetowymi serwisami społecznościowymi, usługami platform udostępniania wideo, towarzyszami AI, ogólnymi chatbotami konwersacyjnymi, grami internetowymi i sklepami z aplikacjami lub też z działań innych użytkowników na platformie lub w systemach.

(2) Powołano specjalny panel ekspertów ds. bezpieczeństwa dzieci w internecie („specjalny panel”), aby doradzał Komisji w sprawie europejskiego podejścia do bezpieczeństwa dzieci w internecie. W lipcu 2026 r. przedstawiono sprawozdanie współprzewodniczących specjalnego panelu, opierające się na sześciu podstawowych zasadach: podejście uwzględniające rozwój, równość i różnorodność, ochrona małoletnich, publicznie odpowiedzialne usługi cyfrowe i prawa konsumentów,

[1] Dz.U. C, , s..
[2] Dz.U. C, , s..

wzmocnienie pozycji i edukacja medialna oraz prawa i uczestnictwo dzieci. W sprawozdaniu zalecono w szczególności ogólnounijne ograniczenia dostępu do mediów społecznościowych, zharmonizowane zasady uwzględniania bezpieczeństwa na etapie projektowania w odniesieniu do mediów społecznościowych, innych usług cyfrowych, gier internetowych i niektórych systemów AI dostępnych dla małoletnich, a także proporcjonalne, chroniące prywatność systemy potwierdzania wieku. Celem jest objęcie całego środowiska cyfrowego, aby zapewnić skuteczną i kompleksową ochronę małoletnich w internecie (media społecznościowe+).

(3) Państwa członkowskie w coraz większym stopniu wprowadzają przepisy krajowe ustanawiające minimalny wiek dostępu małoletnich do niektórych usług online lub rozważają wprowadzenie takich przepisów. Biorąc pod uwagę z natury transgraniczny charakter internetu oraz usług i systemów internetowych, takie rozbieżne przepisy krajowe mają negatywny wpływ na rynek wewnętrzny, który zgodnie z art. 26 TFUE obejmuje obszar bez granic wewnętrznych, zapewniający swobodny przepływ towarów i usług oraz swobodę przedsiębiorczości. Warunki ograniczania przez dostawców dostępu małoletnich do niektórych usług i systemów, a także obowiązki dotyczące projektowania usług i systemów wymagają harmonizacji, tak aby zagwarantować pewność prawa dostawcom oferującym usługi i systemy dostępne dla małoletnich w całej Unii oraz zapewnić zharmonizowany poziom ochrony małoletnich niezależnie od ich lokalizacji w Unii.

(4) W rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2065[3] ustanowiono horyzontalne ramy obowiązków w zakresie należytej staranności dla dostawców usług pośrednich, w tym szczególne obowiązki dotyczące ochrony małoletnich w internecie. W szczególności w art. 28 wspomnianego rozporządzenia zobowiązano dostawców platform internetowych dostępnych dla małoletnich do wprowadzenia odpowiednich i proporcjonalnych środków w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w ramach usług świadczonych przez takich dostawców. W wytycznych Komisji dotyczących środków służących zapewnieniu wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w internecie[4] określono niewyczerpujący wykaz środków, które dostawcy platform internetowych dostępnych dla małoletnich powinni wprowadzić w celu wypełnienia obowiązku wynikającego z art. 28 ust. 1 rozporządzenia (UE) 2022/2065.

(5) Niniejsze rozporządzenie doprecyzowuje i uzupełnia odpowiednie przepisy rozporządzenia (UE) 2022/2065 w odniesieniu do ochrony małoletnich, w szczególności w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich, z uwzględnieniem wytycznych i sprawozdania sporządzonego przez współprzewodniczących specjalnego panelu. W tym celu w niniejszym rozporządzeniu określono zasady dotyczące zharmonizowanego minimalnego wieku wymaganego do założenia konta w internetowych serwisach społecznościowych, usługach platform udostępniania wideo, a także zasady dotyczące zharmonizowanych wymogów w zakresie projektowania takich usług oraz potwierdzania wieku.

---

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.U. L 277 z 27.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

[4] Komunikat Komisji – Wytyczne dotyczące środków służących zapewnieniu wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w internecie na podstawie art. 28 ust. 4 rozporządzenia (UE) 2022/2065 (Dz.U. C, C/2025/5519, 10.10.2025, ELI: http://data.europa.eu/eli/C/2025/5519/oj).

(6) W związku z powyższym przepisy ustanawiające zharmonizowany minimalny wiek wymagany do założenia konta w internetowych serwisach społecznościowych i usługach platform udostępniania wideo, zharmonizowane wymogi bezpieczeństwa dla internetowych serwisów społecznościowych, usług platform udostępniania wideo, usług platform gier wideo i sklepów z aplikacjami oraz zharmonizowane zasady dotyczące potwierdzania wieku online i odpowiedzialności rodzicielskiej, w zakresie, w jakim wprowadzają one w życie obowiązek wprowadzenia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich, stanowią uszczegółowienie przepisów art. 28 rozporządzenia (UE) 2022/2065.

(7) Żadnego z przepisów niniejszego rozporządzenia nie należy interpretować jako nałożenia ogólnego obowiązku monitorowania ani ogólnego obowiązku aktywnego ustalania faktów, ani też jako nałożenia na dostawców usług pośrednich ogólnego obowiązku podejmowania aktywnych działań w odniesieniu do nielegalnych treści.

(8) Niniejsze rozporządzenie uzupełnia również rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689[5], w którym określono kompleksowe, oparte na analizie ryzyka ramy regulacji sztucznej inteligencji w Unii. Rozporządzenie (UE) 2024/1689 zakazuje niektórych praktyk związanych ze sztuczną inteligencją, w tym wykorzystywania podatności małoletnich na zagrożenia w sposób wyrządzający szkodę i manipulacji. Ponadto określono w nim wymogi dotyczące systemów AI wysokiego ryzyka, wymogi dotyczące przejrzystości interaktywnych i generatywnych systemów AI oraz obowiązki dostawców najbardziej zaawansowanych modeli AI ogólnego przeznaczenia w zakresie oceny i ograniczania ryzyka systemowego, w tym ryzyka dla bezpieczeństwa i dobrostanu małoletnich. Bez uszczerbku dla wymogów i obowiązków określonych w rozporządzeniu (UE) 2024/1689 niniejsze rozporządzenie ma na celu przeciwdziałanie szczególnym zagrożeniom, jakie stwarzają dla małoletnich towarzysze AI i ogólne chatboty konwersacyjne, oraz określenie zharmonizowanych środków, jakie dostawcy tych systemów AI powinni przyjąć, aby zapewnić wysoki poziom ochrony zdrowia i bezpieczeństwa małoletnich oraz wspierać ich dobrostan i rozwój fizyczny, psychiczny i emocjonalny.

(9) Niniejsze rozporządzenie należy postrzegać jako część ogólnych wysiłków UE na rzecz ochrony użytkowników, w tym dzieci i innych grup szczególnie wrażliwych, przed narażeniem na nielegalne treści w internecie. Wysiłki te obejmują dyrektywę (UE) 2024/1385 w sprawie zwalczania przemocy wobec kobiet i przemocy domowej, która kryminalizuje udostępnianie bez zgody intymnych obrazów lub zmanipulowanych materiałów, nawoływanie do nienawiści ze względu na płeć, cybermolestowanie i cyberstalking, w tym wymierzone w małoletnich.

(10) Niniejsze rozporządzenie pozostaje bez uszczerbku dla przepisów określonych w dyrektywie 2010/13/UE regulujących inne aspekty świadczenia usług objętych niniejszym rozporządzeniem, w szczególności przepisów dotyczących ochrony małoletnich jako widzów treści audiowizualnych. W przypadku gdy inne instrumenty prawa Unii regulują podobne, ale nie bardziej szczegółowe aspekty świadczenia usług objętych zakresem niniejszego rozporządzenia, pierwszeństwo powinno mieć niniejsze rozporządzenie.

---

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

(11) Opierając się na definicjach dotyczących środowiska cyfrowego, niniejsze rozporządzenie powinno mieć zastosowanie do niektórych usług społeczeństwa informacyjnego rozumianych zgodnie z definicją w dyrektywie (UE) 2015/1535 Parlamentu Europejskiego i Rady, tj. każdej usługi normalnie świadczonej za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy. W szczególności niniejsze rozporządzenie powinno mieć zastosowanie do dostawców internetowych serwisów społecznościowych i usług platform udostępniania wideo. Niniejsze rozporządzenie powinno mieć również zastosowanie do niektórych systemów AI w rozumieniu art. 3 ust. 1 rozporządzenia (UE) 2024/1689, które są dostępne dla małoletnich i które kwalifikują się jako towarzysze AI lub ogólne chatboty konwersacyjne. Ponadto niniejsze rozporządzenie powinno mieć zastosowanie do dostawców systemów operacyjnych zdefiniowanych w rozporządzeniu (UE) 2022/1925, a także do dostawców sklepów z aplikacjami zdefiniowanych w rozporządzeniu 2022/1925, które są rodzajem usługi pośrednictwa internetowego skupiającej się na aplikacjach jako produkcie lub usłudze będących przedmiotem pośrednictwa. Aby uniknąć wątpliwości, niniejsze rozporządzenie ma również zastosowanie do tych internetowych serwisów społecznościowych, platform udostępniania wideo i sklepów z aplikacjami, które wskazano jako bardzo duże platformy internetowe na podstawie art. 33 rozporządzenia (UE) 2022/2065.

(12) Gry wideo stały się ważną częścią środowiska cyfrowego, w którym małoletni uczestniczą i wchodzą w interakcję z innymi osobami w sposób oparty na zabawie, ukierunkowany na osiąganie celów lub zapewniający rozrywkę. Niektóre platformy gier wideo umożliwiają rozpowszechnianie i wymianę treści tworzonych przez użytkowników wśród nieokreślonej liczby odbiorców usługi oraz ułatwiają kontakty między tymi odbiorcami. Takie gry internetowe wchodzą w zakres definicji platform internetowych, o której mowa w rozporządzeniu (UE) 2022/2065, i powinny być objęte zakresem niniejszego rozporządzenia. Jednocześnie niektóre gry internetowe, które nie pozwalają na rozpowszechnianie informacji wśród nieokreślonej liczby odbiorców, powinny również wchodzić w zakres niniejszego rozporządzenia. Obejmuje to każdą grę, w którą można grać na komputerze, urządzeniu mobilnym lub konsoli do gier, niezależnie od tego, czy oprogramowanie będące podstawą gry jest następnie wykonywane lokalnie czy zdalnie, na przykład za pomocą trwałego nośnika, i niezależnie od tego, czy usługa jest świadczona nieodpłatnie, odpłatnie czy za wynagrodzeniem hybrydowym obejmującym zakupy w ramach usługi (lub aplikacji). Gry internetowe, które są dostępne lub można je kupić wyłącznie za pośrednictwem nośników fizycznych, bez żadnego komponentu online umożliwiającego dostęp do nich, ich dystrybucję lub zakup, nie są uznawane za gry internetowe do celów niniejszego rozporządzenia. Aby uniknąć wątpliwości, w przypadku gdy gra internetowa ma również pewne funkcje odpowiadające platformie udostępniania wideo, uznaje się ją za grę internetową do celów niniejszego rozporządzenia.

(13) Aby zapewnić proporcjonalność niniejszego rozporządzenia, nie powinno ono mieć zastosowania do usług lub systemów, które ze względu na swój niekomercyjny, edukacyjny, naukowy lub leżący w interesie publicznym charakter stwarzają zasadniczo bardzo niskie ryzyko dla małoletnich. Wyłączenie to powinno obejmować nienastawione na zysk encyklopedie internetowe, nienastawione na zysk repozytoria, usługi i systemy edukacyjne i naukowe, które zostały zaprojektowane głównie do celów edukacyjnych i są obsługiwane przez placówki lub organizacje edukacyjne lub na ich rzecz, platformy, usługi i systemy opracowywania i udostępniania otwartego oprogramowania specjalnie stworzone i obsługiwane wyłącznie do celów badań naukowych i rozwoju oraz usługi i systemy zaprojektowane, rozwijane i obsługiwane

przez organy publiczne i do wyłącznego użytku tych organów publicznych lub w ich imieniu.

(14) W przypadku gdy dostawcy usług objętych zakresem niniejszego rozporządzenia podlegają również obowiązkowi zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony zgodnie z art. 28 ust. 1 rozporządzenia (UE) 2022/2065, obowiązki te określa się w odniesieniu do kwestii objętych niniejszym rozporządzeniem. Wypełnianie obowiązków określonych w niniejszym rozporządzeniu nie powinno być jednak interpretowane jako wystarczające samo w sobie, aby stanowić dowód przestrzegania przez takich dostawców art. 28 ust. 1 rozporządzenia 2022/2065, i w związku z tym powinno pozostawać bez uszczerbku dla dalszych środków zmniejszających ryzyko, które tacy dostawcy mogą być zobowiązani wprowadzić w odniesieniu do kwestii nieobjętych niniejszym rozporządzeniem, na przykład kwestii związanych z zapewnieniem ochrony. Podobnie art. 28 ust. 1 rozporządzenia (UE) 2022/2065 powinien mieć nadal zastosowanie do platform internetowych nieobjętych zakresem niniejszego rozporządzenia.

(15) Do celów niniejszego rozporządzenia należy ustanowić wspólną definicję „małoletniego” lub „dziecka”. „Małoletniego” lub „dziecko” należy rozumieć jako każdą osobę fizyczną w wieku poniżej 18 lat, niezależnie od jakichkolwiek przepisów prawa krajowego przewidujących wcześniejsze lub późniejsze osiągnięcie pełnoletności. Ponadto, chociaż dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, sklepów z aplikacjami i systemów AI pozostają w głównej mierze odpowiedzialni za bezpieczeństwo swoich usług i systemów w przypadku korzystania z nich przez małoletnich, rodzice i opiekunowie prawni mogą odgrywać rolę w kształtowaniu doświadczeń małoletnich w internecie. Pojęcie opiekuna do celów niniejszego rozporządzenia powinno opierać się na definicji odpowiedzialności rodzicielskiej zawartej w rozporządzeniu Rady (UE) 2019/1111[6].

(16) Do celów niniejszego rozporządzenia stosuje się definicję „systemu AI” określoną w art. 3 pkt 1 rozporządzenia (UE) 2024/1689. Należy ponadto zdefiniować niektóre rodzaje systemów AI, które kwalifikują się jako towarzysze AI lub ogólne chatboty konwersacyjne i podlegają uzupełniającym obowiązkom wynikającym z niniejszego rozporządzenia. W przypadku odniesienia w niniejszym rozporządzeniu do dostawcy towarzysza AI lub ogólnego chatbota konwersacyjnego, pojęcie „dostawcy” należy rozumieć zgodnie z definicją w art. 3 pkt 3 rozporządzenia (UE) 2024/1689.

(17) Definicje odnoszące się do potwierdzania wieku, w tym „weryfikacji wieku”, „potwierdzania wieku”, „unijnej listy dostawców unijnych poświadczeń dowodu wieku”, „unijnej listy dostawców unijnych rozwiązań z zakresu weryfikacji wieku”, „unijnego systemu weryfikacji wieku” i „poświadczenia dowodu wieku”, należy rozumieć jako oparte na unijnych ramach ustanowionych rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 zmienionym rozporządzeniem (UE) 2024/1183, a także na zaleceniu Komisji (UE) 2026/1035 z dnia 29 kwietnia 2026 r. w sprawie ustanowienia wspólnych ram dla ogólnounijnych technologii weryfikacji wieku oraz na powiązanych wytycznych Komisji w sprawie ochrony małoletnich w internecie, a także jako spójne z tymi ramami.

---

[6] Rozporządzenie Rady (UE) 2019/1111 z dnia 25 czerwca 2019 r. w sprawie jurysdykcji, uznawania i wykonywania orzeczeń w sprawach małżeńskich i w sprawach dotyczących odpowiedzialności rodzicielskiej oraz w sprawie uprowadzenia dziecka za granicę (Dz.U. L 178 z 2.7.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/1111/oj).

(18) Aby zagwarantować wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, ważne jest, aby obowiązki te były skutecznie stosowane i nie były obchodzone. W związku z tym dostawcy nie powinni dopuszczać się zachowań, które mogłyby podważyć skuteczność obowiązków ustanowionych w niniejszym rozporządzeniu. Takim zachowaniem może być projekt usługi lub systemu, przedstawianie odbiorcom usługi lub użytkownikom systemu 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. Na przykład nie należy wymagać od małoletnich podczas tworzenia konta obniżania poziomu ustawień dotyczących danych wrażliwych, takich jak dostęp do geolokalizacji lub kamery. Nie należy ich również nakłaniać do obchodzenia obowiązków związanych z odroczonym dostępem. Dostawcy powinni również ograniczać tworzenie przez małoletnich dodatkowych kont mających na celu obejście środków bezpieczeństwa uwzględnianych na etapie projektowania.

(19) Aby usługi, z których korzystają małoletni, zapewniały najwyższy poziom prywatności, bezpieczeństwa i ochrony, dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo, którzy zostali wskazani jako bardzo duże platformy internetowe wyznaczone zgodnie z art. 33 rozporządzenia (UE) 2022/2065, powinni powiadomić Komisję o środkach, które zamierzają wprowadzić w celu zapewnienia skutecznego wypełniania obowiązków, takich jak odroczony dostęp do usług i uwzględnianie bezpieczeństwa na etapie projektowania. Powinno to umożliwić Komisji sprawdzenie, po przeprowadzeniu oceny przez niezależnych audytorów posiadających szczególną wiedzę fachową, czy dostawcy podlegający obowiązkom określonym w rozdziałach II–V niniejszego rozporządzenia podjęli środki niezbędne do wypełnienia tych obowiązków. Komisja powinna zareagować na taki plan zapewnienia zgodności, bez uszczerbku dla swoich uprawnień w zakresie nadzoru i egzekwowania przepisów, w szczególności uprawnień do wszczynania postępowań na podstawie art. 34 niniejszego rozporządzenia. Ten mechanizm powiadamiania jest konieczny i proporcjonalny do celu, jakiemu służy, i przestrzega podstawowych praw do wolności prowadzenia działalności gospodarczej zapisanych w art. 16 Karty oraz wolności otrzymywania i przekazywania informacji na mocy jej art. 11.

(20) Lata 0–15 są szczególnie ważne dla rozwoju poznawczego, emocjonalnego i społecznego małoletnich, a także dla rozwoju ich osobowości, tożsamości i systemów wartości. Dowody naukowe wskazują, że niektóre internetowe serwisy społecznościowe i usługi platformy udostępniania wideo stwarzają szczególnie poważne zagrożenie dla prywatności, bezpieczeństwa i ochrony małoletnich w wieku poniżej 15 lat ze względu na ich konkretne funkcje i funkcjonalności. Badania wskazują na wpływ na zdrowie psychiczne i szczególną podatność dzieci w wieku poniżej 13 lat na zagrożenia, od zagrożeń związanych z biernym korzystaniem z internetu przez dzieci w wieku poniżej 3 lat, kiedy czas spędzany przed ekranem może zastępować opiekę, wpływając na zdolność koncentracji, przyswajanie języka oraz rozwój społeczno-emocjonalny dzieci, poprzez ryzyko niedostosowania ciągłej ekspozycji na bodźce zewnętrzne do rozwijających się zdolności dzieci i kształtującego się postrzegania przez nie samych siebie, aż po ryzyko wzmożonego narażenia na konkretne treści i interakcje promowane przez mechanizmy platform na podstawie wrażliwości rozwojowych. Do ukończenia 15. roku życia nastolatki stopniowo się usamodzielniają, a w miarę jak nadzór ze strony opiekunów i nauczycieli staje się mniej skuteczny, zagrożenia wynikają w coraz większym

stopniu ze społecznego charakteru usług cyfrowych, a nie z indywidualnych zachowań, przy czym nastolatki w wieku od 13 do 15 lat znajdują się w szczególnie krytycznej fazie rozwojowej. Dlatego też kluczowe jest zapewnienie, aby małoletni mogli korzystać z prawa do rozwoju i samostanowienia bez narażenia na istotne skutki, jakie ryzyko i szkody związane z niektórymi usługami internetowymi mogą powodować w ich przypadku. Aby zapewnić równy poziom ochrony małoletnich znajdujących się w Unii, konieczne jest wprowadzenie ogólnounijnego ograniczenia dostępu do mediów społecznościowych+ dla dzieci poniżej 13. roku życia. Aby uniknąć fragmentacji rynku wewnętrznego w wyniku rozbieżnych przepisów krajowych, należy ustanowić zharmonizowany minimalny wiek 15 lat, od którego dozwolone jest tworzenie niezależnych kont w ramach internetowych serwisów społecznościowych i usług platformy udostępniania wideo, które mają funkcje lub funkcjonalności szczególnie szkodliwe dla małoletnich poniżej tego wieku. Powinno to pozostawać bez uszczerbku dla przepisów Unii lub przepisów krajowych zgodnych z prawem Unii, ustanawiających wyższy minimalny wiek dla określonych kategorii treści, takich jak treści pornograficzne lub treści związane z grami hazardowymi.

(21) Funkcje i funkcjonalności, które uznaje się za stwarzające zagrożenie dla prywatności, bezpieczeństwa i ochrony małoletnich w wieku poniżej 15 lat, odpowiadają uznanym na całym świecie klasyfikacjom zagrożeń w internecie, w tym narażenia małoletnich na treści lub kontakty nieodpowiednie do wieku, a także na szkodliwe zachowania innych użytkowników lub inne zagrożenia handlowe lub przekrojowe, takie jak nadmierne korzystanie. Obejmują one zatem funkcje i funkcjonalności, które umożliwiają korzystanie z niektórych szkodliwych treści i ich rozpowszechnianie, a także szkodliwe interakcje lub zachowania. W szczególności usługi umożliwiające odbiorcom rozpowszechnianie treści w czasie rzeczywistym wśród nieokreślonej liczby osób narażają małoletnich na zagrożenie dla ich prywatności, a także na nieodpowiednie treści, takie jak treści pornograficzne; umożliwienie małoletnim interakcji z nieznanymi użytkownikami naraża ich na ryzyko niewłaściwego kontaktu ze strony dorosłych, ale także na działania krzywdzące lub inne nadużycia ze strony innych użytkowników; automatyczne sugerowanie treści lub kontaktów może narażać małoletnich na szkodliwe treści lub wpadanie w „królicze nory” prowadzące do coraz bardziej szkodliwych treści, a także na ryzyko nawiązania potencjalnie szkodliwych kontaktów z użytkownikami o złych zamiarach; wdrażanie funkcji, projektów interfejsów lub cech, które mogą prowadzić do kompulsywnego lub nadmiernego korzystania, takich jak powiadomienia typu „push” lub niekończące się strumienie treści, naraża małoletniego na ryzyko rozwoju zachowań, które szkodzą jego zdrowiu psychicznemu i dobrostanowi, w tym zachowań uzależniających. Funkcje te są zazwyczaj oferowane wyłącznie odbiorcom usługi, którzy mają do niej dostęp za pośrednictwem konta. Zatem uwzględniając prawo małoletniego do wolności wypowiedzi, proporcjonalne jest odroczenie dostępu do usługi w odniesieniu do tworzenia i korzystania z takich kont, ponieważ korzystanie z tej samej usługi bez konta stwarza mniejsze zagrożenie dla małoletnich.

(22) Uznając rolę rodziców i opiekunów prawnych we wspieraniu stopniowego, samodzielnego i bezpiecznego rozwoju małoletnich w internecie, należy zezwolić dostawcom na wyjątkowe odstępstwo od minimalnego wieku niezależnego dostępu określonego w niniejszym rozporządzeniu, i przyjęcie niższego minimalnego wieku 13 lat, aby umożliwić podmiotowi odpowiedzialności rodzicielskiej założenie konta o ograniczonych funkcjach dla dzieci w wieku od 13 do 15 lat. Takie konto powinno należeć do podmiotu odpowiedzialności rodzicielskiej, a nie małoletniego. Odstępstwo to powinno podlegać weryfikacji odpowiedzialności rodzicielskiej i nie powinno

podważać celu niniejszego rozporządzenia, z uwzględnieniem prawa dzieci do ochrony, prywatności oraz nadrzędnego znaczenia najlepszego interesu dziecka. Ponadto odstępstwo to nie powinno być możliwe, jeżeli dostawcy w warunkach świadczenia usług ograniczają dostęp do swoich usług i korzystanie z nich użytkownikom poniżej minimalnego wieku, który jest wyższy niż 13 lat.

(23) W przypadku gdy usługa platformy udostępniania wideo jest przeznaczona specjalnie dla małoletnich w wieku poniżej 13 lat, opiekun może wyjątkowo umożliwić takiemu małoletniemu dostęp do usługi na warunkach określonych w art. 7, wyłącznie przez konto opiekuna oraz pod jego kontrolą i nadzorem. Taki dostęp kontrolowany przez opiekuna nie wiąże się z utworzeniem konta lub korzystaniem z niego przez małoletniego, a zatem nie jest dostępem za pośrednictwem konta utworzonego dla małoletniego lub przypisanego małoletniemu w rozumieniu art. 6 ust. 1. Dostęp kontrolowany przez opiekuna może być zorganizowany za pomocą ustawień lub profili dostosowanych do potrzeb dziecka w ramach konta opiekuna; takie ustawienia lub profile nie stanowią kont małoletniego.

(24) Żaden z przepisów niniejszego rozporządzenia nie nakłada na żadnego dostawcę obowiązku udostępniania swoich usług małoletnim poniżej 13. roku życia ani nie ma wpływu na warunki świadczenia usług wykluczające takich małoletnich – usługi te nadal w pełni podlegają obowiązkom określonym w niniejszym rozporządzeniu w zakresie zapobiegania dostępowi małoletnich. Wymogi związane z dostosowanym do wieku doświadczeniem w ramach usług platformy udostępniania wideo dotyczą wyłącznie tych usług, których dostawcy dokonali świadomego wyboru, aby oferować środowisko zaprojektowane konkretnie dla dzieci, a wybór ten wiąże się ze spełnieniem rygorystycznych warunków.

(25) Dostosowane do wieku i bezpieczne doświadczenia w internecie mają zasadnicze znaczenie dla ochrony małoletnich, którzy coraz więcej czasu spędzają w internecie. Aby zapewnić małoletnim możliwość korzystania z bezpiecznego środowiska cyfrowego, dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI, ogólnych chatbotów konwersacyjnych i sklepów z aplikacjami powinni wprowadzić odpowiednie i proporcjonalne środki, które zapewnią wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich podczas korzystania z ich usługi lub systemu. Dlatego dostawcy powinni już na etapie projektowania kształtować swoje usługi i systemy nadając priorytet dobrostanowi małoletnich poprzez uwzględnienie od samego początku w projekcie i sposobie funkcjonowania kwestii prywatności, bezpieczeństwa i ochrony, a także dostosowanie tych usług i systemów do rozwoju małoletnich. W przypadku gdy usługa lub system są dostępne bez rejestracji lub uwierzytelnienia, dostawcy powinni domyślnie skonfigurować projekt i ustawienia dla każdego niezarejestrowanego lub nieuwierzytelnionego użytkownika w sposób gwarantujący wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich. Dostawcy powinni odstąpić od tych wymogów dopiero po ustaleniu, że odbiorca lub użytkownik jest osobą dorosłą, korzystając z potwierdzania wieku zgodnie z niniejszym rozporządzeniem.

(26) W odniesieniu do internetowych serwisów społecznościowych i usług platformy udostępniania wideo środki wprowadzane przez dostawców tych usług w celu wypełnienia obowiązków określonych w niniejszym rozporządzeniu powinny zapewniać, aby małoletni, którzy założyli własne konto w celu korzystania z usługi, nadal korzystali z bezpiecznego środowiska cyfrowego. Chociaż środki te ograniczają ryzyko wynikające ze szczególnych funkcji i funkcjonalności takich usług dla

małoletnich w wieku powyżej 15 lat, internetowe serwisy społecznościowe i platformy udostępniania wideo pozostają jednak nieodpowiednie dla małoletnich w wieku poniżej 15 lat. Przestrzeganie tych obowiązków nie powinno zatem wpływać na ogólne ograniczenie dotyczące zakładania przez małoletnich własnego konta poniżej tego wieku.

(27) Niektóre cechy projektowe internetowych serwisów społecznościowych i usług platformy udostępniania wideo mogą wykorzystywać podatność małoletnich na zagrożenia i przyczyniać się do intensywnego lub nadmiernego korzystania z usługi, kompulsywnych wzorców zachowań lub zachowań przypominających uzależnienia, szkodząc tym samym zdrowiu psychicznemu, emocjonalnemu i fizycznemu małoletnich. Takie funkcje mogą obejmować nieprzerwane korzystanie z treści bez skutecznych punktów zatrzymania, automatyczne odtwarzanie, automatyczne przewijanie, automatyczne ponowne odtwarzanie, nieskończone przewijanie, powiadomienia celowo wysyłane w odpowiednio dobranych momentach w celu ponownego przyciągnięcia uwagi, mechanizmy nagradzania zachęcające do wielokrotnego korzystania lub mechanizmy karania odbiorcy usługi za niepowracanie do niej w regularnych odstępach czasu. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo nie powinni zatem narażać małoletnich na manipulacyjne lub perswazyjne cechy projektowe mające głównie na celu maksymalizację zaangażowania, w przypadku gdy funkcje te mogą naruszać prywatność, bezpieczeństwo lub ochronę małoletnich lub podważać ich autonomię. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo nie powinni podważać decyzji małoletniego o zaprzestaniu korzystania z usługi lub braku decyzji o korzystaniu z usługi, stosując np. powiadomienia, które nie są wywołane interakcją małoletniego lub jego działaniem w ramach usługi ani nie są bezpośrednio związane z taką interakcją lub działaniem. Powinno to obejmować sytuacje, w których platforma zmienia zachowanie wobec użytkowników, gdy użytkownicy nie korzystają z usługi. W związku z tym obejmowałoby to funkcje, które mają na celu odzyskanie uwagi użytkownika, takie jak wysyłanie powiadomień o nagrodach za dalsze korzystanie z usługi. Dostawcy nie powinni również zachęcać do zaangażowania w regularnych odstępach czasu lub z większą częstotliwością, w tym poprzez kary lub utratę korzyści za brak zaangażowania się regularnie lub w określonych odstępach czasu. Dostawcy usług powinni wdrożyć dostosowane do wieku narzędzia zarządzania czasem i zwiększania sprawczości użytkowników, w tym widoczne powiadomienia, przypomnienia i inne środki wspierające świadome i celowe korzystanie z usługi, umożliwiające skuteczne przerwanie korzystania z usługi. Ponieważ narzędzia zarządzania czasem są często neutralizowane przez samych małoletnich, dostawcy powinni zapewnić, aby środki te skutecznie ograniczały korzystanie z usługi przez małoletnich i nie były łatwe do obejścia. Takie narzędzia powinny również zapewniać, aby korzystanie z usługi nie wpływało negatywnie na potrzeby małoletnich w zakresie snu. Powinno to obejmować skuteczne uniemożliwianie małoletnim korzystania z usługi w czasie nauki szkolnej i w najważniejszych godzinach snu, które powinny być dostosowane do wieku, zgodnie z zaleceniami naukowymi. Najważniejsze godziny snu należy rozumieć jako okres w nocy, w którym małoletni zwykle śpią, obejmujący co najmniej osiem kolejnych godzin w godzinach 22:00–8:00 czasu lokalnego. Czas nauki szkolnej należy rozumieć jako okres, w którym małoletni najczęściej uczęszczają do szkoły lub w inny sposób uczestniczą w obowiązkowych zajęciach edukacyjnych, zgodnie z mającym zastosowanie prawem krajowym lub praktyką krajową i z zastrzeżeniem dostosowania tego czasu przez opiekunów.

(28) Jednym z najważniejszych elementów projektu i funkcjonowania internetowych serwisów społecznościowych i usług platformy udostępniania wideo jest sposób szeregowania i prezentowania informacji na interfejsie internetowym usługi, który może mieć znaczący wpływ na dostęp małoletnich do informacji, korzystanie z nich i styczność z nimi. Aby zapewnić skuteczną ochronę małoletnich w internecie, dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo, którzy korzystają z systemów rekomendacji, powinni projektować swoje systemy rekomendacji w taki sposób, aby zapewniały one wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich. W tym celu dostawcy powinni stosować wskaźniki oceny, które uwzględniają wyniki w zakresie jakości, bezpieczeństwa i zdrowia psychicznego małoletnich, takie jak wskaźniki mierzące, czy system rekomendacji wybiera i priorytetowo traktuje treści odpowiednie dla wieku i etapu rozwoju małoletniego, oceniające skuteczność systemu w zapobieganiu narażeniu na nielegalne, szkodliwe lub niebezpieczne materiały oraz określające wskaźniki dobrostanu psychicznego w celu oceny wpływu na zdrowie psychiczne małoletnich. Wskaźniki te powinny stanowić podstawę rozważań dotyczących optymalizacji leżących u podstaw projektu celów rekomendacji na platformach internetowych. Aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo powinni przy rekomendowaniu treści traktować priorytetowo wyraźne preferencje użytkowników, takie jak informacje zwrotne od użytkowników i interakcje, które wskazują na wyraźne preferencje użytkowników, zarówno pozytywne, jak i negatywne, w tym deklarowany i celowy wybór tematów będących przedmiotem zainteresowania, ankiety, sprawozdawczość i inne sygnały oparte na jakości. Ponadto, aby zapewnić małoletnim większą sprawczość w odniesieniu do sugerowanych im informacji, dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo powinni domyślnie dezaktywować rekomendacje dotyczące informacji sugerowane przez system rekomendacji na podstawie domyślnych sygnałów opartych na zaangażowaniu pochodzących z zachowania małoletnich w internecie. Przez domyślne sygnały oparte na zaangażowaniu należy rozumieć sygnały i dane, które umożliwiają wnioskowanie o preferencjach użytkowników na podstawie ich działań (zachowanie podczas przeglądania treści na platformie), np. czas poświęcony na oglądanie treści i współczynniki klikalności. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo powinni zapewnić, aby systemy rekomendacji nie polegały na gromadzeniu jakichkolwiek danych osobowych pozyskanych spoza usługi. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo powinni również zapewnić, aby małoletni nie byli narażeni na treści, które są szkodliwe w przypadku wielokrotnego wyświetlania, co należy rozumieć jako obejmujące „królicze nory” lub „bańki filtrujące” treści, które mogą stanowić zagrożenie dla ich bezpieczeństwa i ochrony. Efekt „króliczej nory” odnosi się do stopniowego wzmacniania rekomendacji podobnych treści, co prowadzi odbiorców usługi do niekończących się strumieni treści, które mogą być ekstremalne i szkodliwe dla małoletnich. Efekt „bańki filtrującej” odnosi się do stopniowego wzmacniania treści, w ramach którego małoletni jest w przeważającej mierze narażony na treści lub informacje w sposób ograniczający dostęp do różnorodnych treści lub informacji. Małoletni powinni mieć również możliwość wpływania na swoje systemy rekomendacji i kontrolowania proponowanych treści za pomocą specjalnych narzędzi. Małoletnim należy zaoferować łatwy sposób zresetowania systemów rekomendacji poprzez usunięcie wszystkich wcześniej określonych preferencji oraz możliwość wyboru jednej opcji, która nie opiera się na profilowaniu, niezależnie od tego, czy są

zarejestrowani, czy nie, jak przewidziano w art. 38 rozporządzenia (UE) 2022/2065, i niezależnie od tego, czy dany dostawca jest dostawcą bardzo dużej platformy internetowej zgodnie z art. 33 rozporządzenia (UE) 2022/2065. Aby zapewnić skuteczność takiego środka, dostawcy ci powinni regularnie przypominać małoletnim o możliwości zresetowania głównego strumienia treści i zapewniać, aby opcja ta nie była zaprojektowana w sposób zachęcający małoletnich do wyboru opcji opartej na profilowaniu.

(29) Projektowanie ustawień w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony jest ważne dla zminimalizowania zagrożeń internetowych dla małoletnich poprzez zmniejszenie prawdopodobieństwa narażenia małoletnich na treści, interakcje lub funkcjonalności, które mogą być szkodliwe, w tym w okolicznościach, w których dzieci nie są zarejestrowane w usłudze. W tym celu dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo powinni zapewnić, aby ustawienia, takie jak te, które umożliwiają śledzenie lub lokalizowanie odbiorców usługi, dostęp do mikrofonu, kontaktów i kamery lub rekomendowanie małoletnim innych kont, były domyślnie wyłączone dla małoletnich. Jeżeli są one włączone, niektóre ustawienia uwzględniające ochronę prywatności, takie jak dostęp do lokalizacji, powinny zostać wyłączone po zakończeniu sesji, a w każdym razie małoletni powinni być zawsze informowani, gdy są one aktywowane. Ponadto powiadomienia typu „push” powinny być domyślnie wyłączone i projektowane w sposób, który nie wpływa negatywnie na potrzeby małoletnich w zakresie snu i czasu nauki szkolnej. Dlatego nigdy nie należy wysyłać dzieciom powiadomień typu „push” w czasie nauki szkolnej i w najważniejszych godzinach snu, z wyjątkiem sytuacji, gdy takie powiadomienia dotyczą pilnych ostrzeżeń dotyczących bezpieczeństwa – na przykład związanych z bezpieczeństwem konta – lub kontaktów z opiekunami. Powiadomienia typu „push” to powiadomienia, które pojawiają się na urządzeniu w celu poinformowania odbiorcy usługi o bieżących działaniach w ramach usługi, niezależnie od tego, czy usługa jest aktywnie wykorzystywana, a tym samym służą do zachęcenia użytkowników do dalszego korzystania z usługi. Ponadto w przypadku gdy niektóre ustawienia i funkcje mogą być szczególnie szkodliwe dla małoletnich, dostawcy powinni uniemożliwić małoletnim dostęp do nich. Takimi szkodliwymi funkcjami mogą być filtry szkodzące dobrostanowi psychicznemu małoletnich, na przykład poprzez nieproporcjonalne upiększenie, zniekształcenie lub idealizowanie wizerunku dziecka – z wyłączeniem nieszkodliwych filtrów, takich jak te naśladujące zwierzęta – a także funkcje zwiększające porównania społeczne, takie jak umożliwianie dzieciom zobaczenia liczby reakcji na ich treści.

(30) Jako że sprawcy często korzystają z przestrzeni cyfrowej, aby dotrzeć do dzieci, małoletni powinni być chronieni przed ryzykiem związanym z kontaktem, w tym przed cyberszykanowaniem, molestowaniem, a także przed osobami usiłującymi nagabywać w celach seksualnych, wykorzystywać seksualnie lub szantażować małoletnich, handlarzami ludźmi oraz osobami próbującymi zwerbować małoletnich do gangów przestępczych lub promującymi przemoc, radykalizację, brutalny ekstremizm i terroryzm. W związku z tym interakcje między małoletnimi a niezarejestrowanymi odbiorcami usługi, a także nieznanymi odbiorcami usługi, zwłaszcza dorosłymi, powinny być objęte solidnymi zabezpieczeniami. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo powinni zapewnić, aby informacje o małoletnim, takie jak informacje profilowe, biografia, aktywność, lista znajomych, obserwujących i podobne informacje, nie były domyślnie dostępne dla odbiorców usługi, a w każdym razie dla odbiorców usługi nieposiadających konta. Małoletni powinni mieć możliwość sprawowania skutecznej

kontroli nad widocznością swoich danych osobowych, takich jak zdjęcie profilowe, informacje profilowe, udostępniane treści, kontakty, aktywność i historia lub wszelkie inne dane udostępniane na koncie lub profilu. Dane kontaktowe małoletnich – w tym m.in. adres, adres e-mail i numer telefonu – nie powinny być udostępniane innym odbiorcom usługi. Małoletni powinni mieć możliwość blokowania wszelkich innych odbiorców usługi, zarządzania udostępnianymi treściami oraz regulowania interakcji i powiązanych wskaźników, takich jak polubienia i liczba obserwujących. Domyślnie hosting transmisji strumieniowych na żywo lub innych transmisji w czasie rzeczywistym powinien być uniemożliwiony, podobnie jak dostęp do informacji o koncie małoletniego przez odbiorców usługi, którzy nie zostali wyraźnie zaakceptowani. Aby zapewnić, by możliwość włączenia tych ustawień pozostawała proporcjonalna, powinna ona zależeć od wieku i rozwijających się zdolności małoletniego, na przykład poprzez zapewnienie, aby konta publiczne oraz możliwość prowadzenia transmisji strumieniowych na żywo były dostępne wyłącznie dla dzieci, które ukończyły wymagany minimalny wiek, i wyłącznie za wyraźną zgodą ich opiekuna.

(31) Praktyki handlowe występują w usługach cyfrowych w różnych formach i mogą mieć szczególny wpływ perswazyjny wobec małoletnich, którzy mierzą się z różnorodnymi, dynamicznymi i spersonalizowanymi taktykami, na przykład poprzez reklamy, lokowanie produktu, korzystanie z walut wirtualnych, marketing influencerów, sponsorowanie czy zachęty wzmacniane przez AI. Zgodnie z obowiązującymi horyzontalnymi ramami prawnymi, oraz bez uszczerbku dla ich stosowania, w szczególności z dyrektywą 2005/29/WE Parlamentu Europejskiego i Rady[7], która ma pełne zastosowanie do wszystkich praktyk handlowych, w tym wobec małoletnich jako konsumentów, oraz z przepisami rozporządzenia (UE) 2022/2065 dotyczącymi reklamy (art. 26, art. 28 ust. 2 i art. 39) i zwodniczych interfejsów (art. 25). W szczególnym przypadku zwodniczych interfejsów rozporządzenie (UE) 2022/2065 pełni funkcję „sieci bezpieczeństwa” uzupełniającej dyrektywę 2005/29/WE. Transakcje gospodarcze mogą być szkodliwe dla bezpieczeństwa i ochrony małoletnich korzystających z usługi, zwłaszcza gdy nie rozumieją oni konsekwencji dokonywanych przez siebie transakcji. W związku z tym małoletni powinni być wyraźnie informowani o transakcjach gospodarczych dokonywanych w internecie. W tym celu zakupy dokonywane w ramach usługi powinny być oznaczane jako transakcja gospodarcza w łatwo zrozumiały sposób i w czasie rzeczywistym. Waluty wirtualne i inne tokeny mogą również prowadzić do niepożądanych wydatków, w związku z czym wszystkie rodzaje zakupów powinny być prezentowane w walucie krajowej miejsca zwykłego pobytu małoletniego. Ponadto dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo powinni zapewnić, aby małoletni jako konsumenci podatni na zagrożenia nie byli wyzyskiwani; dostawcy nie powinni też projektować swojej platformy w sposób, który może prowadzić do nadmiernych, impulsywnych lub niepożądanych wydatków. Powinno to obejmować w szczególności wprowadzenie rozdzielenia lub mechanizmów utrudniających dokonywanie zakupu produktów powiązanych z treściami, a także zapobieganie narażeniu małoletnich na „loot boxy” i inne

[7] 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, ELI: http://data.europa.eu/eli/dir/2005/29/oj).

produkty, które oferują losowe lub nieprzewidywalne wyniki lub mają cechy podobne do gier hazardowych.

(32) Biorąc pod uwagę szczególną podatność małoletnich na zagrożenia oraz ryzyko, jakie towarzysze AI i ogólne chatboty konwersacyjne mogą stwarzać dla ich zdrowia, bezpieczeństwa, praw podstawowych i dobrostanu, dostawcy takich systemów AI powinni wdrożyć środki uwzględniające bezpieczeństwo na etapie projektowania dostosowane do szczególnych cech tych systemów i związanego z nimi ryzyka, aby zaoferować małoletnim doświadczenie dostosowane do ich wieku. Zabezpieczenia powinny obejmować bezpieczne ustawienia i zakazy dotyczące uzależniających cech projektowych. Ponadto małoletni nie powinni być narażeni na funkcje systemu wykazujące zachowania lub symulujące emocje lub relacje międzyludzkie, które mogą powodować zależność emocjonalną i inne rodzaje zależności, w tym gdy taka zależność może mieć negatywny wpływ na relacje z innymi ludźmi i rozwój małoletniego. Aby zapobiec gromadzeniu przez takie systemy danych wrażliwych małoletnich i potencjalnemu wzmocnieniu z czasem szkodliwych wzorców interakcji, należy domyślnie wyłączać trwałą pamięć konwersacyjną interakcji z małoletnimi, z wyjątkiem sytuacji, gdy jest to konieczne do ochrony ich bezpieczeństwa. Towarzysze AI i ogólne chatboty konwersacyjne dostępne dla małoletnich powinny również podlegać odpowiednim testom i ocenie przed wprowadzeniem do obrotu lub oddaniem do użytku, a następnie w regularnych odstępach czasu.

(33) Dostawcy towarzyszy AI i ogólnych chatbotów konwersacyjnych dostępnych dla małoletnich powinni również wdrożyć monitorowanie po wprowadzeniu do obrotu w celu zidentyfikowania i ograniczenia zagrożeń dla zdrowia, bezpieczeństwa i praw podstawowych małoletnich oraz ich dobrostanu i rozwoju psychicznego, fizycznego i emocjonalnego oraz w celu oceny skuteczności wprowadzonych środków, chyba że dostawca jest mikroprzedsiębiorstwem lub małym przedsiębiorstwem. W tym kontekście należy pamiętać, że jeżeli towarzysz AI lub ogólny chatbot konwersacyjny opiera się na modelu AI ogólnego przeznaczenia z ryzykiem systemowym, model ten podlega już szczególnym obowiązkom w zakresie zarządzania ryzykiem na podstawie rozporządzenia (UE) 2024/1689. Zarządzanie ryzykiem systemowym przez dostawców tych modeli powinno obejmować ocenę i, w razie potrzeby, zmniejszanie ryzyka dla bezpieczeństwa i dobrostanu małoletnich, w tym ryzyka dla małoletnich wynikającego ze korzystania przez nich z modelu zgodnie z prawem oraz z korzystania z modelu przez inne osoby, które mogą wyrządzić krzywdę małoletnim. W związku z tym właściwe jest, aby odpowiednie środki ograniczające wdrożone w ramach tego zarządzania ryzykiem systemowym zgodnie z art. 55 rozporządzenia (UE) 2024/1689 były wykorzystywane przez dostawców towarzyszy AI i ogólnych chatbotów konwersacyjnych w ramach ich wysiłków na rzecz spełnienia wymogów niniejszego rozporządzenia. Podobnie oceny ryzyka i środki zmniejszające ryzyko wdrożone na podstawie art. 34 i 35 rozporządzenia (UE) 2022/2065 mogą być również brane pod uwagę, jeżeli są stosowane przez dostawcę towarzysza AI lub ogólnego chatbota konwersacyjnego wdrożonego jako funkcja internetowego serwisu społecznościowego lub usługi platformy udostępniania wideo w ramach świadczenia tej usługi. Takich środków zmniejszających ryzyko nie należy jednak uznawać za wystarczające do zapewnienia zgodności z wymogami określonymi w niniejszym rozporządzeniu.

(34) W przypadku gdy towarzysz AI lub ogólny chatbot konwersacyjny jest wdrażany jako funkcjonalność platformy internetowej lub wyszukiwarki internetowej, obowiązki określone w rozporządzeniu (UE) 2022/2065 powinny nadal mieć zastosowanie do

dostawcy tych usług pośrednich, jeżeli spełnione są warunki ich stosowania. W szczególności wdrożenie takich funkcjonalności nie powinno mieć wpływu na stosowanie przepisów dotyczących oceny i zmniejszania ryzyka systemowego, w tym ryzyka wynikającego z projektu, funkcjonowania lub użytkowania tych funkcjonalności, w zakresie, w jakim stanowią one część usługi oferowanej przez platformę internetową lub wyszukiwarkę internetową. Aby zapewnić przejrzystość interakcji z takimi systemami, dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo oraz gier internetowych, którzy w ramach świadczenia swoich usług wykorzystują funkcjonalność towarzyszy AI lub ogólnych chatbotów konwersacyjnych, powinni również wdrożyć środki umożliwiające małoletnim dokonywanie świadomych wyborów dotyczących korzystania z tych towarzyszy lub chatbotów oraz możliwość rezygnacji z takiego korzystania. Powinno to obejmować obowiązki tych dostawców w zakresie zapewnienia, aby małoletni nie byli nakłaniani do korzystania z tych systemów za pomocą technik projektowych, takich jak wyświetlanie towarzyszy AI i ogólnych chatbotów konwersacyjnych na szczycie listy kontaktów małoletniego. Ponadto zabezpieczenia powinny mieć zastosowanie do towarzyszy AI oraz ogólnych chatbotów konwersacyjnych, jeżeli są one wykorzystywane jako funkcjonalność w ramach usługi gry internetowej, w której możliwe jest dokonywanie zakupów w grze.

(35) Gry internetowe mogą przybierać bardzo różne formy; można je podzielić na kategorie takie jak gry akcji, przygodowe, gry fabularne, strategiczne, sportowe, symulacje lub gry logiczne, i są one zazwyczaj uruchamiane na komputerze osobistym, urządzeniu mobilnym lub konsoli. Gry internetowe mogą zapewnić małoletnim, w tym osobom z niepełnosprawnościami, nie tylko rozrywkę, ale również środowiska internetowe do komunikacji i interakcji społecznych. Wieloosobowe gry internetowe umożliwiają małoletnim kontakt z innymi i budowanie więzi społecznych między różnymi grupami wiekowymi i lokalizacjami geograficznymi. Gry internetowe mogą również przyczyniać się do uczenia się przez osoby małoletnie koordynacji, współpracy i przedmiotów takich jak nauki przyrodnicze, matematyka i języki. Platformy gier wideo umożliwiają użytkownikom granie i tworzenie własnych treści lub gier oraz ich publiczne rozpowszechnianie. Zarówno gry wideo, jak i platformy gier wideo mogą stwarzać różne zagrożenia dla małoletnich. Zostało to również podkreślone w sprawozdaniu współprzewodniczących specjalnego panelu ds. bezpieczeństwa dzieci w internecie, w którym stwierdzono, że gry wideo mogą narażać dzieci na szkodliwe praktyki handlowe lub niebezpieczne kontakty, a systemy klasyfikacji wiekowej mogą zapewnić rodzicom i opiekunom orientację i wgląd w ocenę gier.

(36) Biorąc pod uwagę szczególną podatność małoletnich oraz ryzyko, jakie gry internetowe mogą stwarzać dla ich prywatności, bezpieczeństwa i ochrony, dostawcy gier internetowych powinni wdrożyć środki uwzględniające bezpieczeństwo na etapie projektowania dostosowane do szczególnych cech tych gier internetowych i związanego z nimi ryzyka, aby zaoferować małoletnim doświadczenie dostosowane do ich wieku. Takie ryzyko wiąże się w szczególności z niechcianymi próbami nawiązywania kontaktu w grach wideo, treściami nieodpowiednimi do wieku oraz mechanizmami projektowymi, które mogą prowadzić do zachowań uzależniających i nadmiernego korzystania z gier. Jako że sprawcy często korzystają z przestrzeni cyfrowej, aby dotrzeć do dzieci, gry internetowe z otwartą komunikacją narażają małoletnich na zagrożenia związane z kontaktami, w tym związane z cyberszykanowaniem, molestowaniem, a także przed osobami usiłującymi nagabywać w celach seksualnych, wykorzystywać seksualnie lub szantażować małoletnich, handlarzami ludźmi oraz osobami próbującymi zwerbować małoletnich

do gangów przestępczych lub promującymi przemoc, radykalizację, brutalny ekstremizm i terroryzm. Podobnie niektóre ustawienia mogą narażać małoletnich na treści, interakcje lub funkcjonalności, które mogą być szkodliwe, w tym w okolicznościach, w których dzieci nie są zarejestrowane w usłudze. Dostawcy gier internetowych powinni zatem wprowadzić zabezpieczenia zapobiegające wykorzystywaniu usługi do nakłaniania małoletnich do nawiązywania kontaktów w ramach innych usług, które mogą stanowić zagrożenie dla ich prywatności, bezpieczeństwa i ochrony. Można to osiągnąć poprzez ograniczenie przekierowań („link-outs") tam, gdzie może to stanowić zagrożenie dla małoletnich, oraz poprzez wprowadzanie komunikatów ostrzegawczych dla małoletnich. Platformy gier wideo również mogą zwiększać ryzyko styczności małoletnich z treściami nieodpowiednimi do ich wieku. W przypadku gdy platformy gier wideo umożliwiają odbiorcom usługi tworzenie indywidualnych gier wideo, dostawca platformy gier wideo powinien wprowadzić niezbędne oprogramowanie i środki organizacyjne, aby umożliwić dostawcy nowo utworzonej gry wideo przestrzeganie obowiązujących przepisów.

(37) Niektóre cechy projektowe gier internetowych mogą wykorzystywać podatność małoletnich na zagrożenia i sprzyjać intensywnemu lub nadmiernemu korzystaniu z usługi, kompulsywnym wzorcom zachowania lub zachowaniom charakterystycznym dla uzależnień, szkodząc tym samym zdrowiu psychicznemu, emocjonalnemu i fizycznemu małoletnich. Gry internetowe nie powinny zatem posiadać funkcji, które służą zniechęcaniu małoletnich do zaprzestania gry, podważeniu decyzji o niepodejmowaniu gry w grę internetową, lub funkcji bądź mechanizmów nagradzających, które służą zachęcaniu ich do gry w regularnych odstępach czasu lub z większą częstotliwością, w tym poprzez kary lub utratę korzyści za nieregularne granie lub granie w określonych odstępach czasu.

(38) Dostawcy sklepów z aplikacjami znajdują się w wyjątkowej sytuacji, jeśli chodzi o sposób udostępniania odbiorcom usług stwarzających zagrożenie dla małoletnich. Aby zadbać o wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w środowisku internetowym, dostawcy sklepów z aplikacjami powinni wprowadzić system klasyfikacji ze względu na wiek pozwalający ustalić odpowiednie grupy wiekowe, do których mogą być kierowane aplikacje rozpowszechniane w ramach ich usługi. Taki system klasyfikacji ze względu na wiek powinien obejmować wszystkie aplikacje oraz odpowiednio uwzględniać prawa i najlepszy interes dziecka, w tym rozwój zdolności i różne stopnie dojrzałości małoletnich. Dostawcy sklepów z aplikacjami powinni uniemożliwiać małoletnim zakup lub dostęp do aplikacji oznaczonych jako nieodpowiednie dla ich grupy wiekowej. Ponadto, aby zapewnić zgodność z mającym zastosowanie prawem Unii i prawem krajowym przyjętym zgodnie z prawem Unii, w przypadku gdy dostawca sklepu z aplikacjami dowie się, że za pośrednictwem jego usługi rozpowszechniane są aplikacje, które stanowią lub zawierają głównie treści podlegające wymogowi wyższego minimalnego wieku zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym, dostawca nie powinien zezwalać małoletnim poniżej tego minimalnego wieku z tego państwa członkowskiego na dostęp do tych aplikacji lub ich zakup za pośrednictwem jego usługi. W tym celu dostawcy sklepów z aplikacjami powinni oceniać wiek odbiorcy usługi zgodnie z rozdziałem V niniejszego rozporządzenia. W trosce o przejrzystość i interes społeczny, dostawcy sklepów z aplikacjami powinni podawać do wiadomości publicznej, w jasny i przystępny sposób, informacje na temat metodyki, kryteriów i źródeł, na których opierają swoje systemy klasyfikacji ze względu na wiek.

(39) Kodeksy postępowania mogą być ważnym narzędziem ochrony małoletnich w środowisku internetowym. W tym kontekście Komisja powinna zachęcać do opracowywania lub dalszego rozwijania dobrowolnych kodeksów postępowania na szczeblu Unii, ustanawiających wspólne metody i kryteria dla systemów klasyfikacji ze względu na wiek, aby przyczynić się do zharmonizowanego funkcjonowania takich systemów w ramach stosowania niniejszego rozporządzenia, w tym przez dostawców sklepów z aplikacjami. Kodeksy postępowania powinny w szczególności ułatwiać wzajemne uznawanie i spójne stosowanie klasyfikacji ze względu na wiek we wszystkich państwach członkowskich, określać odpowiednie kryteria, metody i źródła informacji na potrzeby oceny stosowności najistotniejszych rodzajów treści w odniesieniu do wieku – w tym treści zawierających przemoc, o charakterze seksualnym, związanych z hazardem i dotyczących samookaleczania, a także zakupów wewnątrz aplikacji, ryzyka kontaktu i uzależniających cech projektowych – a także ustanawiać niezbędne środki zaradcze i mechanizmy dochodzenia roszczeń oraz zapewniać przejrzystość, w połączeniu z regularnym, przejrzystym i niezależnym monitorowaniem i oceną realizacji zamierzonych celów. Przy ustalaniu, czy dostawca usług naruszył obowiązki określone w niniejszym rozporządzeniu, w stosownych przypadkach można wziąć pod uwagę odrzucenie przez danego dostawcę usług, bez odpowiednich wyjaśnień, zaproszenia Komisji do stosowania takiego kodeksu postępowania. Fakt uczestnictwa w danym kodeksie postępowania i jego wdrażania nie powinien sam w sobie oznaczać, że niniejsze rozporządzenie jest przestrzegane. Ogólnoeuropejski system informacji o klasyfikacji gier ze względu na wiek (PEGI) i kodeks postępowania PEGI stanowią punkt odniesienia dla uczestniczących przedsiębiorstw w odniesieniu do oznaczania wieku, promocji i marketingu oraz odzwierciedlają zobowiązanie branży gier wideo do informowania opinii publicznej w odpowiedzialny sposób. Przepisy dotyczące kodeksów postępowania zawarte w niniejszym rozporządzeniu mogłyby służyć jako podstawa dla już podjętych na szczeblu Unii działań współregulacyjnych, które zostałyby zaadaptowane jako kodeks postępowania. Mógłby to być między innymi system klasyfikacji ze względu na wiek PEGI, pod warunkiem że spełniłby wymogi niniejszego rozporządzenia w zakresie dbałości o wysoki poziomu prywatności, bezpieczeństwa i ochrony małoletnich.

(40) Małoletni grający w gry internetowe powinni korzystać z takiej samej ochrony w odniesieniu do transakcji gospodarczych jak w przypadku korzystania z internetowych serwisów społecznościowych i usług udostępniania wideo, w tym z prawa do przejrzystości co do rzeczywistej wartości pieniężnej transakcji przeprowadzanych za pośrednictwem walut wirtualnych, a także do ochrony przed wpływem zmiennych mechanizmów nagradzających, których związek z zachowaniami charakterystycznymi dla hazardu i zachowaniami kompulsywnymi jest dobrze udokumentowany. Kodeksy postępowania w dziedzinie gier internetowych należy oprzeć na utworzonych już ogólnoeuropejskich ramach klasyfikacji i samoregulacji lub systemach klasyfikacji ze względu na wiek funkcjonujących na szczeblu państw członkowskich, w tym na ich niedawno rozszerzonych wersjach obejmujących interaktywne kategorie ryzyka i praktyki monetyzacji, a ramy te należy na bieżąco aktualizować w świetle postępu naukowego i technologicznego oraz pojawiających się zagrożeń dla małoletnich. Przestrzeganie kodeksu postępowania, który Komisja uzna za odpowiedni, może świadczyć o zgodności z wynikającymi z wdrożonych środków obowiązkami określonymi w niniejszym rozporządzeniu, ale nie może stanowić przesłanki do uzyskania odstępstwa od ustanowionych w nim zakazów.

(41) Aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w środowisku cyfrowym, dostawcy usług internetowych serwisów społecznościowych, usług platformy udostępniania wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz gier internetowych powinni na wszystkich etapach projektowania, udoskonalania i świadczenia swoich usług uwzględniać rozwój zdolności i zainteresowań dzieci oraz ich zmieniającą się podatność na zagrożenia. Wdrożone rozwiązania powinny być zatem co najmniej przyjazne dla dziecka, łatwe do zrozumienia i łatwo dostępne dla wszystkich małoletnich, w tym dla osób z niepełnosprawnościami lub dodatkowymi potrzebami w zakresie dostępności. Bardzo duże platformy internetowe w rozumieniu art. 33 rozporządzenia (UE) 2022/2065 muszą przekazywać takie informacje w językach urzędowych państw członkowskich, w których świadczą usługi. Dostawcy usług internetowych serwisów społecznościowych, usług platformy udostępniania wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz gier internetowych powinni również umożliwiać małoletnim przekazywanie informacji zwrotnych na temat treści, wyników wyszukiwania i podsuwanych im podpowiedzi w ramach usługi. Takie informacje zwrotne powinny być uwzględniane oraz mieć istotne przełożenie na lepsze dostosowanie usługi do dzieci. Ponadto małoletni powinni być stopniowo uświadamiani, co oznaczają konkretne ustawienia domyślne oraz uczeni, jak nimi zarządzać. Jeżeli małoletni zmienia ustawienia dotyczące ochrony, dostawca powinien wysłać jasne ostrzeżenia i umożliwić łatwe przywrócenie ustawień, w tym tymczasową zmianę ustawień i powrót do ustawień domyślnych za pomocą jednego kliknięcia. Aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, dostawcy nie powinni wielokrotnie nakłaniać lub zachęcać małoletnich do obniżenia poziomu ochrony.

(42) Aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, konieczne jest wdrożenie skutecznych, widocznych i przyjaznych dziecku mechanizmów zgłaszania oraz mechanizmów ułatwiających małoletnim zgłaszanie treści, kont, grup, funkcji i zachowań, które mogą mieć negatywny wpływ na ich bezpieczeństwo i ochronę prywatności podczas korzystania z usługi. Obejmuje to zgłaszanie kont należących do użytkowników poniżej minimalnego wieku, zgodnie z niniejszym rozporządzeniem. Takie mechanizmy nie powinny mieć wpływu na stosowanie art. 16 rozporządzenia (UE) 2022/2065. Aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, takie mechanizmy powinny, w stosownych przypadkach, umożliwiać małoletnim samodzielne sformułowanie treści zgłoszenia oraz domyślnie ukrywać tożsamość małoletnich przed innymi odbiorcami usługi lub użytkownikami systemu. Zgłoszenia składane przez małoletnich powinny być traktowane priorytetowo. Małoletni powinni ponadto otrzymać potwierdzenie wpłynięcia zgłoszenia wraz z dostosowanymi do wieku informacjami na temat kroków, które zostaną następnie podjęte, orientacyjnymi terminami i możliwymi skutkami. W stosownych przypadkach wszelkie ograniczenia nałożone przez dostawców w następstwie takich zgłoszeń dokonanych przez małoletnich należy uznać za ograniczenia w zakresie widoczności zgodnie z art. 17 ust. 1 lit. a) rozporządzenia (UE) 2022/2065. Małoletni powinni ponadto mieć dostęp do kompleksowego i odpowiedniego wsparcia, jeżeli zetkną się z nielegalnymi i szkodliwymi treściami i działaniami. W tym celu dostawcy usług internetowych serwisów społecznościowych, usług platformy udostępniania wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych oraz usług platform gier wideo powinni udostępniać narzędzia wsparcia, które są łatwo dostępne i dostosowane do potrzeb małoletnich oraz które umożliwiają przekierowanie do krajowych służb wsparcia lub

połączenie z nimi, w tym z centrami bezpieczniejszego internetu, telefonami zaufania dla dzieci i infoliniami, służbami odpowiedzialnymi za ochronę dzieci, a w stosownych przypadkach, udostępniają dane kontaktowe organów ścigania. Te narzędzia wsparcia powinny być również połączone z krajowymi aplikacjami dotyczącymi bezpieczeństwa w internecie, jeżeli takie aplikacje istnieją, takimi jak aplikacja 3018 oferowana przez e-Enfance, a także z europejską aplikacją dotyczącą bezpieczeństwa w internecie, jeżeli jest ona dostępna. Aby sprawić, że małoletni będą świadomi zagrożeń w środowisku internetowym, należy informować ich o konkretnych zagrożeniach, zanim zamieszczą w internecie treści lub zwiększą widoczność niektórych z nich, np. udostępniając treści zamieszczane przez innych odbiorców. W tym celu dostawcy usług internetowych serwisów społecznościowych, usług platformy udostępniania wideo, towarzyszy AI, ogólnych chatbotów konwersacyjnych oraz gier internetowych powinni, w stosownych przypadkach, wdrożyć komunikaty ostrzegawcze lub inne odpowiednie rozwiązania służące informowaniu małoletnich przed podjęciem jakichkolwiek działań.

(43) Opiekunowie odgrywają ważną rolę w życiu małoletnich – pomagają im między innymi w bezpiecznym i świadomym poruszaniu się w środowisku internetowym. Należy zatem ułatwić opiekunom udzielanie takiego wsparcia, udostępniając im narzędzia dla opiekunów. Narzędzia dla opiekunów to oprogramowanie, elementy, funkcje lub aplikacje, które mają pomóc opiekunom monitorować aktywność małoletnich w internecie, ich prywatność, bezpieczeństwo i dobrostan, przy jednoczesnym poszanowaniu sprawczości i prywatności dzieci. Narzędzia dla opiekunów należy uznać za uzupełnienie innych rozwiązań uwzględniających bezpieczeństwo już na etapie projektowania, ale nigdy nie powinny one zwalniać dostawców z odpowiedzialności za zapewnienie wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich. Nadzór rodzicielski nie zawsze jest możliwy ze względu na różne sytuacje życiowe dzieci, opiekunowie mogą być nieobecni lub niezaangażowani, dlatego ciężar zapewnienia zgodności z przepisami nie powinien spoczywać wyłącznie na opiekunach. Narzędzia dla opiekunów powinny obejmować co najmniej funkcje zgłaszania treści w imieniu dziecka, ustalania limitu czasu spędzanego przed ekranem, widoczności kont, z którymi małoletni wchodzi w interakcję, i otrzymywania powiadomień o nich, zarządzania ustawieniami konta, a także inne funkcje umożliwiające nadzorowanie korzystania z usług objętych zakresem niniejszego rozporządzenia, które mogą naruszać prywatność małoletniego, zagrażać jego bezpieczeństwu i obniżać poziom jego ochrony. Takie funkcje mogą obejmować ostrzeżenia, które opiekun otrzymuje, jeżeli istnieje podejrzenie, że w wyszukiwaniach małoletniego powtarzają się tematy samobójstwa, samookaleczenia lub zaburzeń odżywiania lub jeżeli małoletni nawiązał kontakt lub znajomość z innymi kontami, w tym w przypadku gdy takie konta należą do osób dorosłych. W przypadku gdy opiekunowie zarządzają ustawieniami konta małoletniego, powinni mieć możliwość wyboru okresu, na jaki zamierzają zmienić takie ustawienia. Narzędzia te powinny być dostosowane do wieku małoletniego i należycie uwzględniać jego stopniowy rozwój. Narzędzia dla opiekunów powinny być dostosowane do wieku, łatwo dostępne i łatwe do aktywacji, skuteczne i trudne do obejścia, a przy tym funkcjonować z poszanowaniem prawa małoletnich do prywatności, dostępu do informacji i stopniowego usamodzielniania się w miarę rozwoju ich zdolności. Na przykład opiekun powinien móc korzystać z takiego narzędzia bez konieczności utworzenia konta w serwisie, a zmiany w ustawieniach powinny być możliwe wyłącznie po dokonaniu autoryzacji w takim samym zakresie, jaki był wymagany przy pierwszej aktywacji narzędzi. Małoletni powinni być w jasny

sposób informowani o uruchomieniu takich narzędzi i powinni, w szczególności w przypadku aktywnej funkcji monitorowania, otrzymywać jasne powiadomienia w czasie rzeczywistym. Interoperacyjność bardzo dużych platform internetowych w rozumieniu art. 33 ust. 1 rozporządzenia (UE) 2022/2065 z narzędziami dla opiekuna oferowanymi przez podmioty trzecie powinna jeszcze bardziej zwiększyć ich użyteczność i skuteczność, zgodnie z warunkami określonymi w art. 6 rozporządzenia (UE) 2022/1925. Należy przekazać Komisji uprawnienia do przyjmowania zgodnie z art. 290 TFUE aktów uzupełniających niniejsze rozporządzenie poprzez ustanowienie niezbędnych przepisów i kryteriów technicznych dotyczących narzędzi dla opiekunów.

(44) Niektóre podmioty, organizacje i stowarzyszenia dysponują szczególną wiedzą ekspercką i kompetencjami w zakresie wykrywania i sygnalizowania podejrzewanych naruszeń niniejszego rozporządzenia, a ich skargi mogą mieć pozytywny wpływ na wolność wypowiedzi i ogólnie na wolność dostępu do informacji. W związku z tym opiekunowie i małoletni powinni mieć prawo umocować takie podmioty, organizacje lub stowarzyszenia, zgodnie z warunkami określonymi w art. 86 rozporządzenia (UE) 2022/2065, do wykonania w imieniu małoletnich praw przyznanych niniejszym rozporządzeniem. Oprócz prawa do wniesienia skargi zgodnie z art. 53 rozporządzenia (UE) 2022/2065 małoletni i opiekunowie, którzy są odbiorcami usługi i użytkownikami systemów, oraz każdy podmiot, organizacja lub zrzeszenie powinni mieć prawo do wniesienia skargi na dostawców podlegających niniejszemu rozporządzeniu. Takie skargi należy składać do określonego zgodnie z art. 27 właściwego organu państwa członkowskiego, w którym odbiorca usługi ma miejsce zamieszkania lub siedzibę, zgodnie z krajowymi zasadami dobrej administracji. W przypadku towarzyszy AI i ogólnych chatbotów konwersacyjnych należy stosować art. 85 rozporządzenia (UE) 2024/1689. Możliwości zaskarżania decyzji dostawców platform internetowych nie powinny jednak pod żadnym względem naruszać możliwości skorzystania z sądowych środków odwoławczych zgodnie z prawem danego państwa członkowskiego, a tym samym nie powinny wpływać na wykonywanie prawa do skutecznego środka prawnego na mocy art. 47 Karty.

(45) Aby zapewnić wysoki poziom ochrony małoletnich, dostawcy nie tylko wdrażają konkretne rozwiązania, ale również – w przypadku dostawców bardzo dużych platform internetowych – muszą być w stanie wykazać skuteczność rozwiązań wdrożonych zgodnie z rozdziałem III poprzez odpowiednie monitorowanie, testowanie i ocenę, które powinny być częścią ocen ryzyka przeprowadzanych na podstawie art. 34 rozporządzenia (UE) 2022/2065. Na potrzeby tej oceny dostawcy powinni wziąć pod uwagę najbardziej aktualne dostępne informacje oraz wnioski ze źródeł naukowych i akademickich. Aby monitorować i oceniać skuteczność rozwiązań w miarę upływu czasu, dostawcy powinni przechowywać wszystkie dokumenty potwierdzające związane z ich oceną przez co najmniej trzy lata.

(46) W trosce o właściwe stosowanie niniejszego rozporządzenia, Komisja powinna zachęcać do opracowywania, wdrażania, regularnego przeglądu i aktualizowania dobrowolnych kodeksów postępowania na szczeblu Unii z udziałem, w stosownych przypadkach, dostawców usług internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI, ogólnych chatbotów konwersacyjnych, a także właściwych organów, organizacji społeczeństwa obywatelskiego i innych odpowiednich zainteresowanych stron, oraz ułatwiać takie działania. Te kodeksy postępowania powinny określać jasne cele, zawierać szczegółowe zobowiązania i ustalenia dotyczące sprawozdawczości proporcjonalne do

wielkości i zasobów dostawców, a także należycie odzwierciedlać specyfikę danych usług oraz potrzeby i interesy wszystkich stron, w szczególności małoletnich. Po konsultacji z Europejską Radą ds. Usług Cyfrowych i Europejską Radą ds. Sztucznej Inteligencji kwestii leżących w zakresie ich odpowiednich kompetencji Komisja powinna przeanalizować, monitorować i oceniać, czy takie kodeksy są odpowiednim narzędziem do zapewniania zgodności z niniejszym rozporządzeniem.

(47) W celu zapewnienia jasności, prostoty i skuteczności oraz skutecznego stosowania i egzekwowania niniejszego rozporządzenia dostawcy usług internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI i ogólnych chatbotów konwersacyjnych, którzy nie mają siedziby w Unii, powinni wyznaczyć przedstawiciela prawnego w państwie członkowskim, w którym oferują swoje usługi lub systemy. Na potrzeby uproszczenia tego wymogu dostawcy, którzy wyznaczyli już przedstawiciela prawnego na podstawie rozporządzenia (UE) 2022/2065 lub rozporządzenia (UE) 2024/1689, powinni mieć możliwość wypełnienia tego obowiązku poprzez rozszerzenie mandatu tego przedstawiciela na wszystkie kwestie związane z otrzymaniem, przestrzeganiem i egzekwowaniem decyzji wydanych na podstawie niniejszego rozporządzenia.

(48) Biorąc pod uwagę zmieniający się charakter zagrożeń przekrojowych, na które mogą być narażeni małoletni w napędzanym ciągłymi innowacjami świecie cyfrowym, należy przekazać Komisji uprawnienia do przyjmowania zgodnie z art. 290 TFUE aktów zmieniających zakazy dotyczące praktyk, które mają na celu zachęcanie lub co do których można przewidzieć, że będą zachęcać małoletnich do kompulsywnego lub nadmiernego korzystania z usługi, środki zapewniające, aby systemy rekomendacji były projektowane z myślą o wysokim poziomie prywatności, bezpieczeństwa i ochrony małoletnich, ustawienia domyślne zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony kont małoletnich, rozwiązania na rzecz wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w odniesieniu do kontaktów między małoletnimi a innymi odbiorcami usługi, rozwiązania ograniczające widoczność wszelkich informacji udostępnianych przez małoletnich i ich interakcji z innymi odbiorcami usługi, środki zapewniające wysoki poziom ochrony zdrowia, bezpieczeństwa, praw podstawowych i dobrostanu małoletnich, którzy mogą mieć dostęp do towarzyszy AI oraz systemów ogólnych chatbotów konwersacyjnych, rozwiązania zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w grach internetowych oraz rozwiązania dające małoletnim sprawczość. Celem tych zmian jest zapewnienie, aby środki służące uwzględnieniu bezpieczeństwa na etapie projektowania pozostały skuteczne i dotrzymywały kroku praktykom. Takie zmiany powinny ograniczać się do tego, co jest konieczne do zagwarantowania prywatności, bezpieczeństwa i ochrony małoletnich.

(49) Aby zweryfikować, czy osoba, która chce utworzyć konto jako opiekun na rzecz małoletniego, posiada odpowiedzialność rodzicielską, dostawcy powinni mieć możliwość korzystania z sygnałów pochodzących z publicznie dostępnych baz danych na szczeblu państw członkowskich, takich jak sygnały dotyczące edukacji lub publiczne rejestry urodzeń, które potwierdzają, że dana osoba dorosła jest opiekunem danego małoletniego. Ponadto w niektórych przypadkach dostawcy usług mogą już posiadać sygnał, że osoba dorosła jest opiekunem małoletniego, np. w przypadku wcześniejszego korzystania z usługi przez danego małoletniego i odpowiednią osobę dorosłą. Dodatkowo osoby dorosłe powinny mieć możliwość złożenia oświadczenia własnego, że wykonują odpowiedzialność rodzicielską. W przypadku takiego

oświadczenia własnego dostawcy powinni dołożyć należytych starań, aby zweryfikować, czy składająca je osoba dorosła jest opiekunem konkretnego małoletniego. Taka weryfikacja powinna być przeprowadzana z poszanowaniem zasad ochrony danych, w szczególności zasady minimalizacji danych poprzez zastosowanie tzw. dowodu z wiedzą zerową, i nie powinna pociągać za sobą dodatkowego przetwarzania danych osobowych, które umożliwiałoby ustalenie tożsamości lub śledzenie danej osoby dorosłej lub danego małoletniego. Pozostaje to bez uszczerbku dla działań, które dostawca powinien móc podjąć w celu wypełnienia swojego obowiązku wynikającego z art. 18 rozporządzenia (UE) 2022/2065. Należy przekazać Komisji uprawnienia do przyjmowania zgodnie z art. 290 TFUE aktów zmieniających niniejsze rozporządzenie poprzez określenie dowodów i sygnałów odpowiedzialności rodzicielskiej. Komisja powinna mieć możliwość dalszej analizy wymogów technicznych i operacyjnych, które umożliwiłyby wykorzystanie unijnego rozwiązania z zakresu weryfikacji wieku jako narzędzia weryfikacji odpowiedzialności rodzicielskiej.

(50) Ocena wieku użytkownika jest niezbędna do skutecznego wdrożenia obowiązków określonych w niniejszym rozporządzeniu w odniesieniu do: rejestracji w internetowych serwisach społecznościowych i na platformach udostępniania wideo, których dotyczy wymóg minimalnego wieku, dostępu do aplikacji nieodpowiednich do wieku oraz zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich poprzez uwzględnianie bezpieczeństwa na etapie projektowania. Stosowane rozwiązania powinny być: dokładne (dokładność ta powinna być regularnie oceniana na podstawie odpowiednich, jasnych i publicznie dostępnych wskaźników, w rzeczywistych okolicznościach i umożliwiać prawidłowe wskazanie użytkownika spełniającego próg wieku), wiarygodne (aby rozwiązanie było wiarygodne, powinno pochodzić z wiarygodnego źródła, być stale dostępne i funkcjonować w różnych okolicznościach) i solidne (nie powinny być łatwe do obejścia), ale nie powinny być inwazyjne (nie powinny wymagać od odbiorców usługi ujawniania ich tożsamości, dokładnego wieku lub innych danych osobowych, jeżeli ustalenie, że odpowiedni próg wieku został osiągnięty, jest wystarczające) ani dyskryminujące (wybrane rozwiązanie powinno być odpowiednie i dostępne dla wszystkich użytkowników niezależnie od niepełnosprawności, języka, pochodzenia etnicznego, płci, religii i przynależności do mniejszości). Jeżeli rozwiązania w zakresie potwierdzania wieku nie spełniają tych wymogów, uznaje się je za niezgodne z niniejszym rozporządzeniem. Samo oświadczenie własne odbiorców usługi nie jest wystarczającym rozwiązaniem w zakresie potwierdzania wieku do celów zgodności z niniejszym rozporządzeniem i nie powinno samo w sobie być uznawane za odpowiedni ani skuteczny środek, gdy ochrona małoletnich wymaga wiarygodnego określenia wieku.

(51) Wymogi niniejszego rozporządzenia dotyczące potwierdzania wieku powinny pozostawać bez uszczerbku dla stosowania rozporządzenia (UE) 2016/679, w szczególności zasad ograniczenia celu i minimalizacji danych przewidzianych w jego art. 5 ust. 1 lit. b) i c), a także wymogów uwzględniania ochrony danych na etapie projektowania i domyślnej ochrony danych. W szczególności wymogi określone w niniejszym rozporządzeniu nie powinny powodować, że dostawcy usług objętych zakresem niniejszego rozporządzenia będą zachowywać, uzyskiwać lub przetwarzać większą ilości danych osobowych, niż jest to absolutnie niezbędne ze względów technicznych do oceny, czy odbiorca usługi jest małoletni. Ponadto dostawcy usług objętych niniejszym rozporządzeniem nie powinni dalej przetwarzać tych informacji ani łączyć ich z dodatkowymi danymi w żadnym innym celu.

Obowiązki w zakresie ochrony danych powinny mieć zastosowanie zarówno do dostawców usług objętych niniejszym rozporządzeniem, jak i do wszelkich osób trzecich zaangażowanych w potwierdzanie wieku, takich jak dostawcy rozwiązań w zakresie potwierdzania wieku. Aby zapewnić najwyższy poziom prywatności i ochrony danych, stosowane rozwiązania w zakresie potwierdzania wieku powinny opierać się na najnowszej technologii i wykorzystywać tzw. dowód z wiedzą zerową.

(52) Aby uniknąć niepotrzebnych niedogodności dla użytkowników i ograniczyć częstotliwość weryfikacji wieku, dostawcy sklepów z aplikacjami oraz dostawcy usług i systemów podlegających obowiązkom określonym w rozdziale III powinni mieć możliwość przechowywania w odniesieniu do konta sygnału wieku potwierdzającego, że użytkownik osiągnął już określony próg wieku. W przypadku dostawców aplikacji oznacza to, że nie muszą oni weryfikować wieku użytkowników, którzy wykazali już, że osiągnęli próg wieku, próbując uzyskać dostęp do aplikacji lub nabyć aplikacje podlegające temu samemu lub niższemu progowi. Dane osobowe przetwarzane w ramach takiego sygnału wieku powinny być ograniczone do tego, co jest absolutnie niezbędne do osiągnięcia celu, i nie powinny być wykorzystywane do żadnych innych celów.

(53) Potwierdzanie wieku to ogólny termin obejmujący różne metody potwierdzania wieku, w tym zarówno weryfikację wieku, jak i szacowanie wieku. W celu zagwarantowania, że odbiorcy usługi osiągnęli minimalny wiek, lub w przypadku świadczenia usługi przyjaznej dzieciom, dostawcy usług internetowych serwisów społecznościowych lub usług platform udostępniania wideo, objętych wymogiem odroczenia dostępu, powinni wprowadzić odpowiednie rozwiązania z zakresu weryfikacji wieku w momencie tworzenia konta. Aby ułatwić przestrzeganie przepisów i promować godne zaufania, interoperacyjne i chroniące prywatność podejście do weryfikacji wieku w całej Unii, dostawcy powinni stosować wyłącznie unijne rozwiązania z zakresu weryfikacji wieku, które opierają się na unijnym poświadczeniu dowodu wieku o potwierdzonej zgodności z wymogami unijnego systemu weryfikacji wieku ustanowionego w zaleceniu Komisji (UE) 2026/1035 i które są wymienione w unijnej liście unijnych rozwiązań z zakresu weryfikacji wieku i unijnej liście dostawców unijnych poświadczeń dowodu wieku. Unijne rozwiązanie z zakresu weryfikacji wieku, z którego korzystają dostawcy, powinna dostarczać niezależna strona trzecia. Normy i kryteria niezbędne do wysoce skutecznej weryfikacji wieku określono w ramach unijnego systemie weryfikacji wieku, a każda osoba trzecia posiadająca poświadczenie zgodności z tym systemem powinna być uznawana za dostarczającą ważne dowody wieku. Aby zapewnić najwyższy poziom prywatności, bezpieczeństwa, dokładności, wiarygodności i nieinwazyjności, a także w trosce o najwyższy poziom dostawców poświadczeń dowodu wieku i rozwiązań z zakresu weryfikacji wieku, wszelkie rozwiązania z zakresu weryfikacji wieku inne niż unijne rozwiązania z zakresu weryfikacji wieku i unijne poświadczenia dowodu wieku należy uznawać za niespełniające określonych w rozporządzeniu wymogów z zakresu oceny wieku. Unijne rozwiązania z zakresu weryfikacji wieku i unijne poświadczenia dowodu wieku powinny spełniać wymogi unijnego systemu weryfikacji wieku, takie jak stosowanie dowodu z wiedzą zerową w celu zapobiegania śledzeniu tożsamości i możliwości powiązania online. Po tym jak państwa członkowskie ustalą i powiadomią, że dostawcy poświadczeń dowodu wieku i rozwiązań z zakresu weryfikacji wieku spełniają te wymogi, dostawców tych należy umieścić w unijnej liście poświadczeń dowodu wieku i unijnej liście unijnych rozwiązań z zakresu weryfikacji wieku.

(54) Do celów zgodności z wymogami dotyczącymi uwzględniania bezpieczeństwa na etapie projektowania określonymi w rozdziale III dostawcy powinni mieć również możliwość stosowania alternatywnych rozwiązań w zakresie potwierdzania wieku zamiast weryfikacji wieku, jeżeli rozwiązania te zapewniają wysoki poziom dokładności, niezawodności, bezpieczeństwa, solidności, nieinwazyjności, prywatności i niedyskryminacji.

(55) Odbiorcy usług i systemów określonych w ust. 1 i 4, którzy uznają, że wynik procedury potwierdzania wieku jest nieprawidłowy, powinni mieć dostęp do skutecznego wewnętrznego mechanizmu rozpatrywania skarg. Mechanizm ten powinien umożliwiać nieodpłatne składanie skarg drogą elektroniczną, być łatwo dostępny i przyjazny dla użytkownika. Aby zapewnić skuteczne dochodzenie roszczeń, dostawcy powinni rozpatrywać takie skargi z należytą starannością, bezstronnie i bez zbędnej zwłoki. W przypadku gdy dostawca systemu operacyjnego uzyskał, zgodnie z niniejszym rozporządzeniem, sygnał wieku użytkownika, dostawca ten powinien, za zgodą użytkownika, umożliwić udostępnianie tego sygnału wieku dostawcom objętym zakresem niniejszego rozporządzenia, jeżeli jest to niezbędne do zapewnienia zgodności z nim. Nie powinno to prowadzić do przetwarzania żadnych dodatkowych danych innych niż dane absolutnie niezbędne do zapewnienia zgodności z niniejszym rozporządzeniem. Ten obowiązek spoczywający na dostawcach systemów operacyjnych powinien pozostawać bez uszczerbku dla obowiązków dostawców w zakresie oceny i weryfikacji wieku, których celem jest zagwarantowanie, że sygnał wieku uzyskano zgodnie z wymogami określonymi w niniejszym rozporządzeniu.

(56) W trosce o jednolite warunki stosowania unijnego systemu weryfikacji wieku w całej Unii należy powierzyć Komisji uprawnienia wykonawcze do określenia specyfikacji niezbędnych do podstawowego funkcjonowania unijnego systemu weryfikacji wieku, w tym procedur wykazywania i oceny zgodności unijnych rozwiązań z zakresu weryfikacji wieku oraz unijnych poświadczeń dowodu wieku przez organy publiczne.

(57) W trosce o jednolite warunki stosowania alternatywnych rozwiązań w zakresie potwierdzania wieku należy przekazać Komisji zgodnie z art. 290 TFUE uprawnienia do przyjmowania aktów uzupełniających niniejsze rozporządzenie poprzez określenie wymogów i specyfikacji niezbędnych do zapewnienia, aby rozwiązania w zakresie potwierdzania wieku osiągnęły wysoki poziom dokładności, niezawodności, bezpieczeństwa, solidności, nieinwazyjności, prywatności i niedyskryminacji, oraz poprzez określenie wymogów niezbędnych do zapewnienia bezpiecznego, chroniącego prywatność i interoperacyjnego udostępniania sygnałów wieku.

(58) Skuteczne korzystanie z możliwości utworzenia konta rodzicielskiego na rzecz małoletniego oraz skuteczne korzystanie z narzędzi dla opiekunów na mocy niniejszego rozporządzenia wymaga, aby osoby dorosłe posiadające odpowiedzialność rodzicielską miały dostęp do środków niezbędnych do udowodnienia takiej odpowiedzialności rodzicielskiej. Państwa członkowskie powinny być zatem zobowiązane do ustanowienia co najmniej jednego środka elektronicznego chroniącego prywatność, za pomocą którego opiekun może uzyskać i przedstawić poświadczenie odpowiedzialności rodzicielskiej w odniesieniu do małoletniego. Ustanawiając taki środek, państwa członkowskie powinny zadbać o to, aby opierał się on na źródłach autentycznych ustanowionych na mocy prawa krajowego, był bezpłatny dla opiekuna i nie wiązał się z udostępnianiem informacji na temat odpowiedzialności rodzicielskiej usługodawcom lub opinii publicznej poza potwierdzeniem istnienia odpowiedzialności rodzicielskiej. Takie środki elektroniczne

chroniące prywatność powinny być skutecznie dostępne dla wszystkich opiekunów i małoletnich posiadających miejsce zamieszkania na terytorium tych państw, w tym osób z niepełnosprawnościami, osób o ograniczonym dostępie cyfrowym lub ograniczonych umiejętnościach cyfrowych oraz osób znajdujących się w trudnej sytuacji, takich jak rodziny uchodźców i przesiedlone rodziny.

(59) Żaden małoletni nie powinien być pozbawiony ochrony wynikającej z niniejszego rozporządzenia, a opiekun środków do jej wykonywania, ze względu na sytuację administracyjną, społeczną lub pobytową rodziny. Państwa członkowskie powinny zatem zadbać o to, aby na podstawie decyzji lub poświadczeń wydanych przez właściwe organy poświadczenia odpowiedzialności rodzicielskiej mogły uzyskać również rodziny, których sytuacja nie znajduje odzwierciedlenia w zwykłych aktach stanu cywilnego, w tym rodziny uchodźców i przesiedlone rodziny oraz prawnie wyznaczeni opiekunowie małoletnich bez opieki.

(60) Aby weryfikacja wieku w całej Unii była skuteczna, odbiorcy usług muszą mieć dostęp do odpowiednich środków uzyskiwania poświadczenia dowodu wieku. Jeżeli uzyskanie poświadczenia dowodu wieku jest niemożliwe, odbiorcy usług nie mają dostępu do usług tylko dlatego, że nie udostępniono im środków z zakresu weryfikacji wieku. Państwa członkowskie powinny zatem zadbać o to, aby uzyskanie poświadczenia dowodu wieku na ich terytorium było możliwe na różne sposoby, np. poprzez biometryczne dowody tożsamości i paszporty, systemy tożsamości cyfrowej, aplikacje podmiotów trzecich lub osobistą weryfikację wieku. Państwa członkowskie powinny dopilnować, aby uzyskane w ten sposób poświadczenia dowodu wieku pozwalały odbiorcom udowodnić, że osiągnęli progi wieku określone w niniejszym rozporządzeniu. Dotyczy to również poświadczeń dowodu wieku w przypadku młodszych dzieci. Dodatkowo państwa członkowskie powinny zagwarantować bezpłatny dostęp do unijnego rozwiązania z zakresu weryfikacji wieku. Państwa członkowskie powinny wyznaczyć organy publiczne odpowiedzialne za certyfikację unijnych rozwiązań z zakresu weryfikacji wieku i unijnych poświadczeń dowodu wieku. W celu spełnienia tego obowiązku państwa członkowskie powinny przekazać Komisji nazwy i adresy organów publicznych wyznaczonych na ich terytorium, wraz z wszelkimi późniejszymi zmianami, a Komisja powinna podać te informacje do wiadomości publicznej. Państwa członkowskie powinny też bez zbędnej zwłoki powiadomić Komisję o unijnych rozwiązaniach z zakresu weryfikacji wieku i unijnych poświadczeniach dowodu wieku o potwierdzonej zgodności z wymogami unijnego systemu weryfikacji wieku, wraz z odpowiednim certyfikatem zgodności, a także o każdym późniejszym zawieszeniu lub cofnięciu takiego certyfikatu. Aby zagwarantować skuteczne i jednolite stosowanie niniejszego rozporządzenia w całej Unii, certyfikowane unijne rozwiązania z zakresu weryfikacji wieku lub certyfikowane unijne poświadczenia dowodu wieku umieszczone na listach, o których mowa w art. 30 ust. 1, powinny być uznawane przez wszystkie państwa członkowskie. Państwa członkowskie nie powinny zatem ograniczać ani utrudniać stosowania na swoim terytorium unijnego rozwiązania z zakresu weryfikacji wieku, które zostało już umieszczone na liście poprzez wyznaczenie przez inne państwo członkowskie.

(61) Wymogi dotyczące wieku ustanowione w niniejszym rozporządzeniu powinny być skutecznie stosowane zarówno do nowych, jak i istniejących kont. Dostawcy usług i systemów, w odniesieniu do których stosuje się minimalny wiek, powinni zatem ustalić w odpowiednim terminie, czy odbiorcy usług lub użytkownicy systemów posiadający już konta osiągnęli obowiązujący minimalny wiek. Dostawcy nie powinni być zobowiązani do przeprowadzania nowej weryfikacji wieku, jeżeli mogą z dużą

dozą pewności stwierdzić, że mający zastosowanie minimalny wiek został już osiągnięty, w tym, w stosownych przypadkach, na podstawie daty utworzenia istniejącego konta. Ta sama zasada powinna mieć zastosowanie w przypadku, gdy dostawcy są zobowiązani do oceny wieku, aby odróżnić osoby dorosłe od małoletnich i ustalić odpowiedzialność rodzicielską, oraz w przypadku dostawców sklepów z aplikacjami, aby mogli oni uniemożliwić małoletnim nabycie i dostęp do aplikacji, które są nieodpowiednie do ich wieku lub które, na podstawie mającego zastosowanie prawa Unii lub prawa krajowego przyjętego zgodnie z prawem Unii, są aplikacjami z ograniczeniami wiekowymi. Podejście to ma na celu uniknięcie sytuacji, w której wszyscy odbiorcy usługi muszą przechodzić przez procedurę weryfikacji wieku lub potwierdzania wieku, nawet jeśli można z wysokim stopniem pewności stwierdzić, że użytkownik jest osobą dorosłą, na przykład na podstawie wiarygodnych informacji, takich jak dane karty kredytowej uzyskane wcześniej zgodnie z prawem. Wysoki poziom zaufania powinien wynikać z oczekiwanych wyników działań w realnych warunkach w odniesieniu do pełnej bazy użytkowników. Dostawcy bardzo dużych platform internetowych, aby ułatwić skuteczny nadzór nad wdrażaniem przez nich tych wymogów, powinni z wyprzedzeniem określić, w jaki sposób zamierzają spełnić wspomniane wymogi dotyczące istniejących kont oraz, w stosownych przypadkach, w jaki sposób zamierzają powoływać się na odpowiednie wyjątki.

(62) W celu zapewnienia zgodności istniejących kont z wymogami dotyczącymi minimalnego wieku dostawcy bardzo dużych platform internetowych powinni przed upływem sześciomiesięcznego okresu przedłożyć właściwemu organowi szczegółowy plan wdrażania, który potwierdza wymagany wysoki stopień pewności. Plan powinien w związku z tym zawierać schematyczny opis całego procesu wykorzystywanego do określenia wieku obecnych użytkowników, wraz z jasnym opisem każdego narzędzia lub środka technicznego oraz podstawowych zasad podejmowania decyzji. W stosownych przypadkach wybór takiego procesu należy poprzeć solidnymi dowodami na jego efektywność w rzeczywistych warunkach, które to dowody uzyskano ze statystycznie reprezentatywnej próby pełnej bazy użytkowników – przy czym należy wykazać reprezentatywność tej próby pod kątem istotnych sygnałów wieku – oraz przedstawić dane dotyczące dokładności, precyzji i czułości procesu w odniesieniu do małoletnich odbiorców, a także pełną macierz pomyłek z uwzględnieniem szczegółowych przedziałów wiekowych, wraz z opisem sposobu pozyskania próby i przypisania oznaczeń wieku. Jeżeli rok utworzenia konta uznaje się za przesłankę do odstępstwa, w planie należy dodatkowo przedstawić dowody empiryczne i pewność statystyczną, że ten pojedynczy sygnał jest wystarczający, aby stwierdzić, że użytkownik osiągnął mający zastosowanie minimalny wiek. W planie należy również określić, w jaki sposób dostawca będzie monitorować, czy osiągnięto oczekiwane wyniki, na przykład poprzez audyt przeprowadzany po wdrożeniu. W planie należy ponadto wykazać, że proponowane środki są zgodne z ogólnymi zasadami potwierdzania wieku określonymi w niniejszym rozporządzeniu, w tym że są dokładne, wiarygodne, bezpieczne, solidne, nieinwazyjne, chroniące prywatność i niedyskryminujące.

(63) Uznając, że skuteczna ochrona małoletnich wymaga nie tylko środków regulacyjnych, ale także zwiększania świadomości, edukacji i upodmiotowienia, państwa członkowskie powinny ustanowić krajowe strategie w oparciu o komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Cyfrowa dekada dla dzieci i młodzieży: nowa europejska strategia na rzecz lepszego internetu dla dzieci (BIK+)” z 11 maja 2022 r. oraz w oparciu o sieci centrów bezpieczniejszego internetu Komisji, uwzględniając

w tych strategiach działania informacyjne, telefony zaufania dla dzieci, opiekunów i wychowawców oraz infolinie do zgłaszania potencjalnie nielegalnych treści w internecie. W szczególności państwa członkowskie powinny promować rozwój umiejętności cyfrowych małoletnich, tak aby w momencie osiągnięcia przez nich minimalnego wieku byli oni w stanie zrozumieć zagrożenia związane ze środowiskiem internetowym objęte niniejszym rozporządzeniem, bezpiecznie i krytycznie korzystać z usług i systemów cyfrowych oraz świadomie korzystać z zabezpieczeń, ustawień i narzędzi, które dostawcy są zobowiązani udostępnić. Małoletni i ich opiekunowie powinni mieć łatwy, bezpłatny i poufny dostęp na szczeblu krajowym do kanałów, za pośrednictwem których małoletni mogą zwrócić się o pomoc w związku z negatywnymi skutkami, o których mowa w niniejszym rozporządzeniu, w tym niechcianym kontaktem i cyberszykanowaniem zgodnie z komunikatem Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Plan działania przeciwko cyberszykanowaniu „Bezpieczniejsi w internecie, razem silniejsi" z 10 lutego 2026 r. Kanały te powinny uzupełniać narzędzia zgłaszania i wsparcia przewidziane w niniejszym rozporządzeniu, oferować szybką pomoc i wskazywać małoletnim inne źródła wsparcia dostępne na szczeblu krajowym. Należy przewidzieć możliwość wspierania tych działań, w tym działań prowadzonych przez centra bezpieczniejszego internetu, za pomocą finansowania unijnego udostępnianego w ramach odpowiednich programów i instrumentów unijnych ustanowionych na podstawie wieloletnich ram finansowych, takich jak plany partnerstwa krajowego i regionalnego. W trosce o skuteczne wdrażanie, państwa członkowskie powinny informować Komisję o podejmowanych działaniach, a Komisja powinna ułatwiać wymianę najlepszych praktyk między państwami członkowskimi.

(64) W niniejszym rozporządzeniu należy uszczegółowić niektóre przepisy rozporządzenia (UE) 2022/2065. W celu zapewnienia skutecznego nadzoru i egzekwowania niniejszego rozporządzenia rozdział IV rozporządzenia (UE) 2022/2065 powinien mieć zastosowanie w zakresie, w jakim odpowiednie przepisy regulują dostawców usług pośrednich objętych zakresem tego rozporządzenia. Komisja powinna mieć wyłączne uprawnienia do nadzoru wykonywania i egzekwowania określonych w niniejszym rozporządzeniu obowiązków, które mają zastosowanie do dostawców bardzo dużych platform internetowych w rozumieniu art. 33 rozporządzenia (UE) 2022/2065.

(65) Podobnie, aby uniknąć powielania działań i zapewnić spójność z obowiązującymi ramami horyzontalnymi, które mają zastosowanie do systemów AI na podstawie rozporządzenia (UE) 2024/1689, egzekwowanie szczególnych wymogów bezpieczeństwa przewidzianych w niniejszym rozporządzeniu w odniesieniu do towarzyszy AI i ogólnych chatbotów konwersacyjnych powinno opierać się na ramach i procedurach nadzoru i egzekwowania określonych w rozporządzeniu (UE) 2024/1689.

(66) Dostawcy gier internetowych będących platformami gier wideo podlegają nadzorowi i procedurom egzekwowania przepisów w ramach struktur ustanowionych na podstawie rozporządzenia (UE) 2022/2065. W trosce o spójność tych struktur ze sposobem egzekwowania przepisów na mocy niniejszego rozporządzenia, właściwy organ odpowiedzialny za nadzór nad dostawcami gier internetowych będących grami wideo powinien być właściwy dla państwa członkowskiego, w którym dostawca ma główną siedzibę.

(67) Aby zapewnić pewność prawa i spójne stosowanie przepisów w całej Unii oraz uniknąć fragmentacji rynku wewnętrznego w wyniku rozbieżnych interpretacji krajowych, organy państw członkowskich nie powinny przyjmować decyzji sprzecznych z decyzją podjętą przez Komisję na podstawie niniejszego rozporządzenia. Komisja, koordynatorzy ds. usług cyfrowych i właściwe organy, w stosownych przypadkach, powinny ściśle współpracować i koordynować swoje działania w zakresie egzekwowania przepisów, tak aby były one spójne, skuteczne i wzajemnie się uzupełniały w odniesieniu do egzekwowania niniejszego rozporządzenia, z jednej strony, oraz rozporządzeń (UE) 2022/2065 i 2024/1689, z drugiej strony, w tym poprzez wykorzystanie mechanizmów współpracy i spójności ustanowionych w rozdziale IV rozporządzenia (UE) 2022/2065.

(68) Komisja powinna dążyć do przyjęcia ostatecznej decyzji w ciągu 90 dni od wszczęcia postępowania w sprawie podejrzenia naruszenia niniejszego rozporządzenia. Powinna również przekazać swoje wstępne ustalenia zainteresowanemu dostawcy usług w terminie 30 dni od wszczęcia postępowania.

(69) Komisja powinna dysponować wszelkimi zasobami, takimi jak zasoby ludzkie, wiedza specjalistyczna czy środki finansowe, niezbędnymi do realizacji swoich zadań wynikających z niniejszego rozporządzenia. Aby zapewnić dostępność zasobów niezbędnych do odpowiedniego nadzoru na poziomie Unii na podstawie niniejszego rozporządzenia, Komisja powinna pobierać roczną opłatę nadzorczą, której poziom należy ustalać co roku, od dostawców usług internetowych serwisów społecznościowych, usług platformy udostępniania wideo, sklepów z aplikacjami oraz towarzyszy AI i ogólnych chatbotów konwersacyjnych, w odniesieniu do których Komisja posiada kompetencje do nadzorowania ich zgodności z rozdziałami II–V niniejszego rozporządzenia i które wskazano jako bardzo duże platformy internetowe na podstawie art. 33 rozporządzenia (UE) 2022/2065. Roczną opłatę nadzorczą wymaganą od tych dostawców na potrzeby egzekwowania niniejszego rozporządzenia należy włączyć do opłaty nadzorczej pobieranej od takich dostawców bardzo dużych platform internetowych na podstawie art. 43 rozporządzenia (UE) 2022/2065. Podobnie jak w przypadku tej opłaty nadzorczej zewnętrzne dochody przeznaczone na określony cel wynikające z rocznej opłaty nadzorczej pobieranej na podstawie niniejszego rozporządzenia powinny pokrywać koszty dodatkowych zasobów ludzkich w Komisji, w tym urzędników, pracowników kontraktowych i ekspertów krajowych. Ponadto pułap opłaty nadzorczej wprowadzony w niniejszym rozporządzeniu należy rozpatrywać wraz z pułapem określonym w rozporządzeniu (UE) 2022/2065 i dostosować jego wysokość tak, aby ogólne zasoby Komisji były wystarczające do wykonywania zadań powierzonych jej na podstawie niniejszego rozporządzenia i rozporządzenia (UE) 2022/2065.

(70) Całkowita kwota rocznej opłaty nadzorczej pobieranej na podstawie niniejszego rozporządzenia powinna obejmować koszty związane z wykonywaniem przez Komisję szczególnych uprawnień i zadań w zakresie nadzoru, monitorowania, prowadzenia dochodzeń i egzekwowania przepisów w odniesieniu do dostawców bardzo dużych platform internetowych i wyszukiwarek internetowych objętych niniejszym rozporządzeniem. W szczególności opłata powinna pokrywać koszty związane z ustanowieniem, utrzymaniem i funkcjonowaniem unijnego systemu weryfikacji wieku, w tym finansowanie działań dotyczących stopniowego wdrażania unijnego rozwiązania z zakresu weryfikacji wieku w całej UE oraz rozwoju wiedzy eksperckiej i zdolności zgodnie z art. 36. Indywidualna roczna opłata nadzorcza nie powinna jednak przekraczać ogólnego pułapu dla każdego dostawcy bardzo dużych

platform internetowych, przy uwzględnieniu możliwości finansowych dostawcy wskazanej usługi lub usług.

(71) Pobierając roczną opłatę nadzorczą na podstawie niniejszego rozporządzenia, Komisja powinna stosować przepisy i zasady określone w art. 43 rozporządzenia (UE) 2022/2065.

(72) Uwzględniając, jak ważna jest ochrona dzieci, Komisja, we współpracy z koordynatorami ds. usług cyfrowych i Radą ds. Usług Cyfrowych, powinna rozwijać wiedzę ekspercką i zdolności Unii w zakresie nadzoru nad usługami objętymi zakresem niniejszego rozporządzenia.

(73) Biorąc pod uwagę znaczenie wpływu usług i systemów objętych zakresem niniejszego rozporządzenia na ochronę małoletnich, niezapewnienie przez dostawców wysokiego poziomu prywatności, bezpieczeństwa i ochrony oraz niewywiązanie się z mających do nich zastosowanie szczególnych obowiązków może w krótkim czasie poważnie wpłynąć na znaczną liczbę małoletnich, którzy korzystają z ich usług lub systemów w różnych państwach członkowskich, i spowodować znaczne szkody, przy czym takie uchybienia mogą być również szczególnie trudne do zidentyfikowania i usunięcia w odpowiednim czasie. Komisja, we współpracy z właściwymi organami, powinna rozwijać wiedzę ekspercką i zdolności Unii, w tym tworzyć sieci wymiany wiedzy, aby szybko reagować na takie incydenty mające wpływ na ochronę małoletnich. Incydent należy rozumieć jako szybko zmieniającą się sytuację w UE lub poza nią, o wymiarze internetowym i domniemanym związku z zakresem niniejszego rozporządzenia, która poważnie i negatywnie wpływa na prywatność, bezpieczeństwo, ochronę lub zdrowie i dobrostan małoletnich korzystających z usługi w Unii i która wymaga natychmiastowej reakcji, np. niebezpieczne lub szkodliwe wyzwania krążące wśród małoletnich i stwarzające dla nich bezpośrednie zagrożenie. Z tego też względu Komisja powinna mieć możliwość koordynowania działań i korzystania z wiedzy eksperckiej i zasobów właściwych organów, na przykład poprzez stałe lub tymczasowe analizowanie konkretnych tendencji lub problemów pojawiających się w odniesieniu do szybko zmieniających się realiów, które wpływają na zdrowie, dobrostan, prywatność, bezpieczeństwo i ochronę małoletnich. Państwa członkowskie powinny współpracować z Komisją przy rozwijaniu takich zdolności, w tym w stosownych przypadkach poprzez oddelegowanie personelu, oraz zaangażować się na rzecz stworzenia wspólnych unijnych zdolności nadzorczych, a także porozumienia administracyjnego określającego procedury ułatwiające szybkie reagowanie w przypadku incydentu mającego wpływ na ochronę małoletnich. Państwa członkowskie powinny ustanowić minimalne poziomy gotowości organów krajowych w celu zapewnienia regularnych kanałów komunikacji między odpowiednimi organami krajowymi a stronami trzecimi oraz w stosownych przypadkach zmapować obowiązujące protokoły reagowania na incydenty na szczeblu krajowym.

(74) Niniejsze rozporządzenie nie narusza praw podstawowych, w tym praw dziecka, uznanych w Karcie praw podstawowych ani praw podstawowych stanowiących ogólne zasady prawa Unii. W związku z powyższym niniejsze rozporządzenie należy interpretować i stosować zgodnie z tymi prawami podstawowymi, w tym prawem do poszanowania życia prywatnego i rodzinnego zapisanym w art. 7 Karty, prawem do ochrony danych osobowych zapisanym w art. 8 Karty, prawem do wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów, zapisanym w art. 11 Karty, prawem do niedyskryminacji zapisanym w art. 21 Karty oraz prawem do przestrzegania praw dziecka zapisanym w art. 24 Karty. Wykonując uprawnienia określone w niniejszym rozporządzeniu, wszystkie zaangażowane organy publiczne

powinny dążyć – w sytuacjach, w których występuje konflikt odpowiednich praw podstawowych – do osiągnięcia właściwej równowagi między danymi prawami zgodnie z zasadą proporcjonalności.

(75) Ponieważ cele niniejszego rozporządzenia, mianowicie przyczynianie się do prawidłowego funkcjonowania rynku wewnętrznego oraz zapewnienie wysokiego poziomu prywatności, bezpieczeństwa i ochrony dzieci, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, gdyż działając samodzielnie, nie mogą one osiągnąć niezbędnej harmonizacji i współpracy, natomiast ze względu na zakres terytorialny i podmiotowy możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(76) Zgodnie z art. 42 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia [DATA] r.

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I – PRZEPISY OGÓLNE

Artykuł 1 – Przedmiot

Niniejsze rozporządzenie przyczynia się do właściwego funkcjonowania rynku wewnętrznego i zapewnia wysoki poziom ochrony małoletnich w internecie w Unii, ponieważ ustanawia zharmonizowane przepisy dotyczące bezpiecznego dla małoletnich i zwiększającego ich podmiotowość środowiska internetowego, w tym zasady ochrony konsumentów. Doprecyzowuje ono i uzupełnia rozporządzenie (UE) 2022/2065 oraz uzupełnia rozporządzenie (UE) 2024/1689. W szczególności niniejsze rozporządzenie określa:

a) ujednolicony minimalny wiek wymagany do zakładania kont w internetowych serwisach społecznościowych i usługach platformy udostępniania wideo;

b) zharmonizowane wymogi bezpieczeństwa w odniesieniu do internetowych serwisów społecznościowych, usług platformy udostępniania wideo, platform gier wideo i sklepów z aplikacjami oraz zharmonizowane wymogi bezpieczeństwa w celu ochrony małoletnich w internecie w odniesieniu do gier wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych;

c) zharmonizowane przepisy dotyczące potwierdzania wieku w internecie.

Artykuł 2 – Zakres

1. Niniejsze rozporządzenie ma zastosowanie do dostawców następujących usług lub systemów dostępnych dla małoletnich:

   a) internetowe serwisy społecznościowe;

   b) usługi platformy udostępniania wideo;

   c) sklepy z aplikacjami

   d) gry internetowe;

e) systemy operacyjne;

f) towarzysze AI;

g) ogólne chatboty konwersacyjne.

2. W odniesieniu do usług, o których mowa w ust. 1 lit. a)–e), niniejsze rozporządzenie ma zastosowanie do dostawców usług niezależnie od ich miejsca prowadzenia działalności, w przypadku gdy oferują oni te usługi odbiorcom usług, którzy mają siedzibę lub znajdują się w Unii.

3. W przypadku systemów AI, o których mowa w ust. 1 lit. f) i g), niniejsze rozporządzenie ma zastosowanie do dostawców wprowadzających do obrotu lub oddających do użytku w Unii takie systemy AI, niezależnie od tego, gdzie dostawcy ci mają siedzibę lub gdzie się znajdują.

4. Niniejsze rozporządzenie nie ma zastosowania do dostawców:

a) niekomercyjnych encyklopedii internetowych;

b) niekomercyjnych repozytoriów edukacyjnych i naukowych;

c) usług i systemów zaprojektowanych głównie do celów edukacyjnych i obsługiwanych przez placówki lub organizacje edukacyjne lub w ich imieniu;

d) platform do tworzenia i udostępniania otwartego oprogramowania, chyba że sama platforma stanowi system AI objęty zakresem niniejszego rozporządzenia lub rozporządzenia (UE) 2024/1689;

e) usług i systemów tworzonych i oddawanych do użytku wyłącznie do celów badań naukowych i prac rozwojowych;

f) usług i systemów zaprojektowanych, opracowanych i obsługiwanych przez organy publiczne i do wyłącznego użytku tych organów publicznych lub w ich imieniu.

5. W przypadku gdy jest to uzasadnione z uwagi na potencjalne ryzyko dla prywatności, bezpieczeństwa i ochrony małoletnich stwarzane przez usługę lub system lub gdy usługa lub system stwarza takie ryzyko, które jest równoważne ryzyku stwarzanemu przez usługi lub systemy, o których mowa już w ust. 4, lub mniejsze od tego ryzyka, Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 40 w celu zmiany ust. 4 niniejszego artykułu poprzez dodanie innych rodzajów usług lub systemów do wykazu usług lub systemów objętych wyłączeniem lub usunięcie usług lub systemów z tego wykazu.

6. Dostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo i platform gier wideo podlegających przepisom art. 28 ust. 1 rozporządzenia (UE) 2022/2065, którzy wypełniają obowiązki określone w niniejszym rozporządzeniu, uznaje się za spełniających wymogi tego artykułu w odniesieniu do kwestii objętych niniejszym rozporządzeniem, w tym w odniesieniu do systemów AI, które są wdrażane jako funkcjonalności platform internetowych objętych zakresem art. 28 ust. 1 rozporządzenia (UE) 2022/2065 w ramach świadczenia tej usługi.

7. Niniejsze rozporządzenie pozostaje bez uszczerbku dla przepisów ustanowionych w innych aktach prawnych Unii regulujących inne aspekty świadczenia usług pośrednich i w ustawodawstwie unijnym mającym zastosowanie do systemów AI na rynku wewnętrznym, w tym w:

a) dyrektywie 2010/13/UE[8];

b) prawie Unii dotyczącym ochrony konsumentów i bezpieczeństwa produktów, w tym w dyrektywach 2005/29/WE, 2011/83/UE, (UE) 2019/770, dyrektywie Rady 93/13/EWG oraz rozporządzeniach (UE) 2019/1020, (UE) 2023/988 i (UE) 2024/1689;

c) prawie Unii dotyczącym ochrony danych osobowych, w szczególności w rozporządzeniu (UE) 2016/679 i dyrektywie 2002/58/WE;

d) dyrektywie (UE) 2024/1385[9].

Artykuł 3 – Definicje

1. Do celów niniejszego rozporządzenia stosuje się definicje „platformy internetowej", „odbiorcy usługi", „interfejsu internetowego", „systemu rekomendacji" określone w art. 3 rozporządzenia (UE) 2022/2065.

2. Do celów niniejszego rozporządzenia stosuje się definicje „internetowego serwisu społecznościowego", „usługi platformy udostępniania wideo" i „sklepu z aplikacjami" określone w art. 2 rozporządzenia (UE) 2022/1925. Do celów niniejszego rozporządzenia usługi te uznaje się za „platformę internetową" w rozumieniu art. 3 lit. i) rozporządzenia (UE) 2022/2065.

3. Do celów niniejszego rozporządzenia stosuje się definicje „systemu AI" i „systemu AI ogólnego przeznaczenia" określone w rozporządzeniu (UE) 2024/1689; definicja „dostawcy" określona w art. 3 pkt 3 tego rozporządzenia ma zastosowanie do systemów AI regulowanych niniejszym rozporządzeniem.

4. Do celów niniejszego rozporządzenia stosuje się definicję „systemu operacyjnego" określoną w art. 2 pkt 1 rozporządzenia delegowanego (UE) 2022/1925.

5. Do celów niniejszego rozporządzenia stosuje się następujące dodatkowe definicje:

a) „małoletni" lub „dziecko" oznacza każdą osobę fizyczną poniżej 18. roku życia;

b) „opiekun" oznacza każdą osobę, na której spoczywa odpowiedzialność rodzicielska za małoletniego zgodnie z mającym zastosowanie prawem krajowym;

c) „towarzysz AI" oznacza system AI, w tym system AI ogólnego przeznaczenia, który zapewnia trwałą, spersonalizowaną interakcję lub towarzystwo, symulujące lub ułatwiające relacje społeczne, emocjonalne lub interpersonalne z użytkownikiem;

d) „ogólny chatbot konwersacyjny" oznacza system AI ogólnego przeznaczenia z ogólnymi funkcjami konwersacyjnymi umożliwiającymi bezpośrednią interakcję z użytkownikami, który jest w stanie udzielić pomocy w wielu

[8] 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, ELI: http://data.europa.eu/eli/dir/2010/13/oj).

[9] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1385 z dnia 14 maja 2024 r. w sprawie zwalczania przemocy wobec kobiet i przemocy domowej (Dz.U. L z 24.5.2024, s. 1, ELI: http://data.europa.eu/eli/dir/2024/1385/oj).

dziedzinach i zadaniach; definicja ta nie obejmuje systemów AI, których funkcja konwersacyjna jest ograniczona do specjalistycznej usługi, zadania lub z góry określonego zestawu funkcji, w tym specjalistycznej obsługi klienta, prowadzenia przedsiębiorstwa, wsparcia technicznego oraz zastosowań sztucznej inteligencji do celów transakcyjnych, edukacyjnych, związanych z wyszukiwaniem informacji, przemysłowych lub produkcyjnych;

e) „gry internetowe” oznaczają gry wideo lub platformy gier wideo;

f) „gra wideo” oznacza usługę społeczeństwa informacyjnego w rozumieniu art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535, która umożliwia odbiorcom usługi angażowanie się za pomocą aplikacji dostępnej lokalnie lub zdalnie, w tym za pomocą trwałego nośnika, i która obejmuje interakcję z interfejsem użytkownika lub urządzeniem wejściowym w celu generowania wizualnych informacji zwrotnych z wyświetlacza w symulowanym środowisku do celów zabawy lub rozrywki;

g) „platforma gier wideo” oznacza „platformę internetową” w rozumieniu art. 3 lit. i) rozporządzenia (UE) 2022/2065, która obejmuje interakcję z interfejsem użytkownika lub urządzeniem wejściowym w celu generowania wizualnych informacji z urządzenia wyświetlającego w symulowanym środowisku [do celów zabawy lub rozrywki];

h) „weryfikacja wieku” oznacza proces lub system służący ustaleniu z wysokim stopniem pewności, czy odbiorca lub użytkownik systemu lub usługi osiągnął określony wiek lub próg wiekowy, na podstawie informacji pochodzących z dokumentów identyfikacyjnych lub innych wiarygodnych i zweryfikowanych źródeł identyfikacji;

i) „potwierdzanie wieku” oznacza zestaw metod, które można stosować do określania, szacowania lub weryfikacji wieku osoby fizycznej, obejmujący szacowanie wieku i weryfikację wieku oraz wykluczający oświadczenie własne odbiorców usługi;

j) „sygnał wieku” oznacza wszelkie dane, atrybuty, tokeny, dane uwierzytelniające lub inne informacje udostępniane, przekazywane lub generowane w celu ustalenia, weryfikacji lub wykazania określonego wieku, progu wiekowego lub przedziału wiekowego danej osoby;

k) „unijne rozwiązanie z zakresu weryfikacji wieku” oznacza rozwiązanie w zakresie weryfikacji wieku, które spełnia wymogi unijnego systemu weryfikacji wieku i jest certyfikowane przez organ publiczny oraz wpisane na unijną listę unijnych rozwiązań z zakresu weryfikacji wieku po powiadomieniu przez państwo członkowskie;

l) „unijna lista dostawców unijnych poświadczeń dowodu wieku” oznacza sporządzoną i opublikowaną przez Komisję listę dostawców wydających unijne poświadczenia dowodu wieku;

m) „unijna lista unijnych rozwiązań z zakresu weryfikacji wieku” oznacza sporządzoną i opublikowaną przez Komisję listę unijnych rozwiązań z zakresu weryfikacji wieku certyfikowanych jako zgodne z unijnym systemem weryfikacji wieku i zgłoszonych przez państwa członkowskie;

n) „unijny system weryfikacji wieku” oznacza schemat poświadczania atrybutów w rozumieniu art. 2 pkt 4 rozporządzenia wykonawczego Komisji (UE)

2025/1569 obejmujący zasady mające zastosowanie do dostawców unijnych rozwiązań z zakresu weryfikacji wieku i unijnych poświadczeń dowodu wieku, ich zatwierdzania i włączania do unijnej listy dostawców unijnych poświadczeń dowodu wieku oraz certyfikacji unijnych rozwiązań z zakresu weryfikacji wieku w celu włączenia ich do unijnej listy unijnych rozwiązań z zakresu weryfikacji wieku;

o) „poświadczenie dowodu wieku" oznacza elektroniczne poświadczenie atrybutów w rozumieniu art. 3 pkt 44 rozporządzenia (UE) nr 910/2014, które umożliwia uwierzytelnienie faktu, że jego posiadacz osiągnął określony wiek, próg wiekowy lub przedział wiekowy;

p) „narzędzia dla opiekunów" oznaczają oprogramowanie, funkcje, funkcjonalności lub aplikacje, które mają pomagać opiekunom w monitorowaniu aktywności internetowej małoletnich w celu zapewnienia im prywatności, bezpieczeństwa i dobrostanu.

Artykuł 4 – Przeciwdziałanie obchodzeniu przepisów

Dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, sklepów z aplikacjami, systemów operacyjnych, towarzyszy AI i ogólnych chatbotów konwersacyjnych:

a) nie mogą dopuszczać się zachowań, które w jakikolwiek sposób utrudniają skuteczne wypełnianie ich odpowiednich obowiązków wynikających z niniejszego rozporządzenia, niezależnie od tego, czy zachowanie to ma charakter umowny, handlowy, techniczny lub jakikolwiek inny lub czy polega na stosowaniu technik behawioralnych lub projektowaniu interfejsu;

b) mają zakaz świadomego i celowego podejmowania wszelkich innych działań, których celem lub skutkiem jest, bezpośrednio lub pośrednio, obejście ich odpowiednich obowiązków wynikających z niniejszego rozporządzenia, aby uniknąć wywiązania się z tych obowiązków.

Artykuł 5 – Zgłoszenie planu zapewnienia zgodności i jego niezależny audyt

1. W terminie 4 miesięcy od powiadomienia o decyzji wskazującej ich jako bardzo dużą platformę internetową na podstawie art. 33 rozporządzenia (UE) 2022/2065 dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo, które zostały wskazane jako bardzo duże platformy internetowe na podstawie art. 33 rozporządzenia (UE) 2022/2065, zgłaszają Komisji plan zapewnienia zgodności opisujący szczegółowo wypełnienie obowiązków określonych w rozdziałach II–V niniejszego rozporządzenia.

   W przypadku dostawców, o których mowa w akapicie pierwszym, już wskazanych jako bardzo duże platformy internetowe na podstawie art. 33 rozporządzenia (UE) 2022/2065, takie powiadomienie następuje w ciągu 30 dni od daty rozpoczęcia stosowania niniejszego rozporządzenia.

   Do dokumentów potwierdzających te zgłoszenia stosuje się odpowiednio art. 34 ust. 3 rozporządzenia (UE) 2022/2065.

2. Aby umożliwić Komisji ocenę przestrzegania przez dostawców, o których mowa w ust. 1, obowiązków określonych w rozdziałach II–V, dostawcy ci zlecają na własny koszt audyt planu zapewnienia zgodności zgłoszonego zgodnie z ust. 1,

przeprowadzany przez co najmniej jednego niezależnego audytora. Niezależni audytorzy posiadają wiedzę fachową lub korzystają z usług ekspertów posiadających udokumentowaną wiedzę fachową w następujących dziedzinach istotnych dla ochrony małoletnich:

a) ochrona praw dziecka;

b) medycyna pediatryczna i psychiatria dziecięca;

c) nauka o rozwoju człowieka;

d) potwierdzanie wieku;

e) projektowanie interfejsów internetowych i systemów rekomendacji;

f) ochrona i bezpieczeństwo danych.

3. Art. 37 ust. 2 i 3 rozporządzenia (UE) 2022/2065 stosuje się odpowiednio do audytów przeprowadzanych na podstawie niniejszego artykułu oraz do niezależnych audytorów i wszelkich ekspertów, z których usług oni korzystają. Koszty audytu ponosi dostawca, którego audyt dotyczy. Koszty te nie przekraczają stawek rynkowych za porównywalne oceny przeprowadzane przez audytorów.

Dostawcy, o których mowa w ust. 1, współpracują z niezależnymi audytorami i zapewniają im dostęp do wszystkich informacji, danych, dokumentów i personelu, istotnych w kontekście przeprowadzanego audytu.

Dostawcy dopilnowują, aby każdy pracownik lub wykonawca, który komunikował się z niezależnym audytorem, był chroniony przed wszelkimi działaniami odwetowymi ze strony dostawcy.

4. Niezależni audytorzy, którym dostawca zlecił zgodnie z ust. 2 przeprowadzenie audytu:

a) oceniają plany zapewnienia zgodności przedłożone przez dostawców na podstawie ust. 1 pod względem obowiązków określonych w rozdziałach II–V;

b) przekazują projekt sprawozdania dostawcy, który może przedstawić uwagi w terminie 15 dni od jego otrzymania;

c) sporządzają sprawozdanie końcowe, uwzględniając wszelkie uwagi otrzymane zgodnie z lit. b), jednocześnie Komisji i dostawcy, w terminie dwóch miesięcy od otrzymania planu zapewnienia zgodności; w sprawozdaniu tym wskazują wszelkie niedociągnięcia w środkach zapewnienia zgodności opisanych w tym planie.

5. Zainteresowany dostawca usług publikuje, bez zbędnej zwłoki po jego otrzymaniu, streszczenie sprawozdania końcowego, o którym mowa w ust. 4 lit. c), niezawierające informacji poufnych.

6. W przypadku gdy Komisja stwierdzi w drodze decyzji na podstawie sprawozdania końcowego, o którym mowa w ust. 4 lit. c), że plan zapewnienia zgodności zawiera niedociągnięcia, zainteresowany dostawca przedkłada Komisji i niezależnemu audytorowi, w terminie 30 dni od otrzymania informacji o decyzji Komisji, plan działań naprawczych określający co najmniej jeden środek naprawczy w odniesieniu do każdego zidentyfikowanego niedociągnięcia.

W planie działań naprawczych dostawca określa również rozsądny termin, który nie może być dłuższy niż 60 dni, na wdrożenie każdego środka naprawczego.

Niezależny audytor weryfikuje wdrożenie środków naprawczych i informuje o tym Komisję oraz zainteresowanego dostawcę.

7. Oceniając wypełnianie przez dostawców, o których mowa w ust. 1, obowiązków określonych w rozdziałach II–V niniejszego rozporządzenia, Komisja jest uprawniona do uwzględnienia planu zapewnienia zgodności, o którym mowa w ust. 1, sprawozdania końcowego, o którym mowa w ust. 4 lit. c), oraz wszelkich środków naprawczych zgłoszonych zgodnie z ust. 6 lub wszelkich innych informacji, które Komisja może uznać za istotne.

8. Ani sprawozdanie końcowe, o którym mowa w ust. 4 lit. c), ani żadne działanie Komisji lub jego brak w odniesieniu do tego sprawozdania końcowego lub planu zapewnienia zgodności nie stanowią stwierdzenia zgodności z obowiązkami określonymi w rozdziałach II–V niniejszego rozporządzenia, ani nie ograniczają uprawnień Komisji wynikających z niniejszego rozporządzenia lub rozporządzenia (UE) 2022/2065.

9. Po pierwszym powiadomieniu na podstawie ust. 1 dostawcy co roku składają sprawozdanie na temat wypełniania obowiązków określonych w rozdziałach II–V niniejszego rozporządzenia w ramach swoich rocznych ocen ryzyka przeprowadzanych zgodnie z art. 34 rozporządzenia (UE) 2022/2065.

   Wypełnianie obowiązków określonych w rozdziałach II–V niniejszego rozporządzenia uwzględnia się w niezależnych audytach przeprowadzanych na podstawie art. 37 rozporządzenia (UE) 2022/2065.

10. Niniejszy artykuł pozostaje bez uszczerbku dla uprawnień Komisji wynikających z niniejszego rozporządzenia i rozporządzenia (UE) 2022/2065, w tym uprawnień do przyjmowania środków tymczasowych.

11. Komisja może przyjmować akty wykonawcze określające wzory i metody na potrzeby audytów przeprowadzanych na podstawie niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą, o której mowa w art. 39.

ROZDZIAŁ II – ODROCZENIE ZAKŁADANIA I KORZYSTANIA Z KONT PRZEZ MAŁOLETNICH W INTERNETOWYCH SERWISACH SPOŁECZNOŚCIOWYCH I USŁUGACH PLATFORMY UDOSTĘPNIANIA WIDEO

SEKCJA I – Odroczenie dostępu małoletnich

Artykuł 6 – Odroczenie zakładania i korzystania z kont

1. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo nie zezwalają osobie fizycznej w wieku poniżej 15 lat na założenie konta w ramach tej usługi ani na dostęp do tej usługi za pośrednictwem konta utworzonego dla tej osoby lub przypisanego do niej, w przypadku gdy usługa ta stwarza zagrożenie dla prywatności, bezpieczeństwa lub ochrony małoletniego poniżej tego wieku.

   Usługę uznaje się za stwarzającą zagrożenie dla prywatności, bezpieczeństwa lub ochrony małoletnich w wieku poniżej 15 lat, jeżeli spełnia ona którykolwiek z następujących warunków:

d) umożliwia odbiorcom, którzy uzyskują dostęp do usługi za pośrednictwem konta, przekazywanie treści w czasie rzeczywistym nieokreślonej liczbie innych odbiorców usługi, m.in. poprzez transmisję strumieniową na żywo treści audiowizualnych;

e) umożliwia odbiorcom, którzy uzyskują dostęp do usługi za pośrednictwem konta, kontaktowanie się, komunikowanie się i inne rodzaje interakcji z innymi odbiorcami usługi, którzy nie należeli wcześniej do sieci kontaktów lub subskrypcji odbiorcy;

f) wykorzystuje system rekomendacji oparty na profilowaniu w rozumieniu art. 4 pkt 4 rozporządzenia (UE) 2016/679;

g) wykorzystuje system rekomendacji sugerujący lub w pierwszej kolejności podsuwający odbiorcy, który uzyskuje dostęp do usługi za pośrednictwem konta, propozycje kontaktów lub informacje, które nie pochodzą z wcześniej istniejącej sieci kontaktów lub subskrypcji odbiorcy;

h) uruchamia lub udostępnia funkcjonalności, rozwiązania interfejsu lub elementy, których celem jest umożliwienie nieprzerwanego korzystania z treści lub w przypadku których można racjonalnie przewidywać, że umożliwią nieprzerwane korzystanie z treści, oraz które zachęcają do interakcji z usługą lub z treścią lub innymi odbiorcami usługi, lub które generują automatyczne powiadomienia mające na celu skłonienie użytkownika do rozpoczęcia lub wznowienia korzystania z usługi.

2. Na zasadzie odstępstwa od ust. 1 dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo mogą zezwalać opiekunom na zakładanie kont dla małoletnich w wieku powyżej 13 lat i poniżej 15 lat z ograniczonymi funkcjami, tak aby umożliwić im dostęp do usługi za pośrednictwem takiego ograniczonego konta. Konta takie spełniają przynajmniej następujące warunki:

a) zawsze uruchamiane są narzędzia dla opiekunów określone w art. 20;

b) opiekunowie mają możliwość ustalenia maksymalnego limitu czasu w ciągu dnia, w którym można uzyskać dostęp do usługi lub systemu za pośrednictwem tego konta; czas ten nie może przekraczać jednej godziny dziennie;

c) opiekunowie mają możliwość zatwierdzania potencjalnych nowych kontaktów i ustalania maksymalnego limitu liczby innych odbiorców lub użytkowników należących do sieci kontaktów konta.

3. Tworząc konto małoletniego zgodnie z ust. 2 niniejszego artykułu, dostawca internetowych serwisów społecznościowych i usług platformy udostępniania wideo podejmuje działania w celu ustalenia, czy osoba tworząca konto jest podmiotem odpowiedzialności rodzicielskiej wobec tego małoletniego zgodnie z art. 26, i weryfikuje, czy odbiorca usługi osiągnął wiek 13 lat zgodnie z art. 28 ust. 1.

4. Przed upływem 6 miesięcy od rozpoczęcia stosowania niniejszego rozporządzenia dostawcy usług objętych zakresem ust. 1 niniejszego artykułu ustalają, czy posiadacze istniejących kont wykorzystywanych do uzyskania dostępu do ich usług ukończyli 15 lat. W przypadku gdy posiadacze istniejących kont mają mniej niż 15 lat, odnośni dostawcy usług wyłączają konta odbiorców lub użytkowników usługi, co do których stwierdzono, że nie osiągnęli tego wieku lub w przypadku których nie można ustalić wieku.

5. W przypadku gdy dostawcy usług objęci zakresem ust. 1 przetwarzają dane osobowe na podstawie art. 6 ust. 1 lit. a) rozporządzenia (UE) 2016/679, przepisy określone w niniejszym artykule powinny mieć zastosowanie równolegle z limitami wiekowymi przewidzianymi w art. 8 tego rozporządzenia.

6. Komisja może przyjmować akty delegowane zgodnie z art. 40 w celu zmiany niniejszego rozporządzenia poprzez modyfikację i uzupełnienie warunków określonych w ust. 1 niniejszego artykułu, aby uwzględnić nowe funkcje i funkcjonalności lub zmiany istniejących funkcji lub funkcjonalności, które stwarzają ryzyko dla prywatności, bezpieczeństwa i ochrony małoletnich w internecie równoważne ryzyku stwarzanemu przez warunki określone w ust. 1 niniejszego artykułu.

Sekcja II – Kontrolowany przez opiekuna dostęp małoletnich poniżej 13. roku życia

Artykuł 7 – Kontrolowany przez opiekuna dostęp dla małoletnich poniżej 13. roku życia

1. Dostawcy usług platformy udostępniania wideo, których usługa jest przeznaczona specjalnie dla małoletnich poniżej 13. roku życia, mogą w drodze wyjątku umożliwić opiekunowi zezwolenie małoletniemu w wieku poniżej 13 lat na ograniczony dostęp do usługi za pośrednictwem konta opiekuna, jeżeli spełnione są wszystkie następujące warunki:

   a) taki dostęp kontrolowany przez opiekuna odbywa się wyłącznie poprzez konto opiekuna i nie tworzy się konta dla małoletniego ani nie przypisuje się mu takiego konta;

   b) dostęp taki jest możliwy i kontrolowany za pomocą narzędzi dla opiekunów, o których mowa w art. 20, lub innych ustawień kontroli rodzicielskiej na koncie opiekuna lub na jego urządzeniu;

   c) dostawca wyraźnie zezwala w swoich warunkach świadczenia usług na dostęp małoletnich poniżej 13. roku życia, jasno określając w nich przedział wiekowy małoletnich, do których dostęp jest dozwolony, pod warunkiem uzyskania zgody opiekunów;

   d) dostawca przeprowadził i opublikował, w co najmniej jednym języku urzędowym państwa członkowskiego i w publicznie dostępnej sekcji swojego interfejsu internetowego, ocenę wpływu usługi lub jej odpowiednich części na małoletnich w określonym przedziale wiekowym, w której to ocenie określił ryzyko i wykazał, w stosownych przypadkach, w jaki sposób skutecznie ograniczono takie ryzyko, z uwzględnieniem odpowiednich grup wiekowych. Spełnienie wymogów określonych w rozdziale III nie skutkuje automatycznie skutecznym ograniczeniem takiego ryzyka;

   e) dostawca określił w jasny i przejrzysty sposób w publicznie dostępnej sekcji swojego interfejsu internetowego, które treści lub zachowania uznaje się w ramach usługi za niedostosowane do wieku lub szkodliwe dla prywatności, bezpieczeństwa i ochrony małoletnich w określonym przedziale wiekowym;

   f) dostępu do treści zidentyfikowanych zgodnie z lit. e) nie udziela się małoletnim poniżej 13. roku życia;

   g) dostępne funkcje i funkcjonalności są dostosowywane i stopniowo dopasowywane do wieku małoletniego zadeklarowanego zgodnie z ust. 4 lit. b);

h) wszystkie funkcje personalizacji i systemy rekomendacji oraz wszelkie funkcjonalności wyszukiwania treści udostępnianych przez innych odbiorców usługi są wyłączone i nie można ich aktywować, chyba że ocena, o której mowa w lit. d), wykaże, że ich aktywacja leży w najlepszym interesie małoletniego i w żaden sposób nie wpływa negatywnie na jego prywatność, bezpieczeństwo i ochronę.

2. Żaden z przepisów niniejszego artykułu nie może być interpretowany jako zobowiązujący dostawcę do umożliwienia dostępu małoletnim poniżej 13. roku życia lub jako przyznający każdemu małoletniemu lub opiekunowi prawo dostępu do usługi, jeżeli warunki nie zezwalają na taki dostęp lub jeżeli dostęp do usługi jest ograniczony do wyższego wieku minimalnego na mocy prawa Unii lub prawa krajowego zgodnego z prawem Unii.

3. Konto, za pośrednictwem którego przyznaje się dostęp kontrolowany przez opiekuna zgodnie z ust. 1, jest tworzone, rejestrowane i prowadzone wyłącznie przez opiekuna. Małoletni uzyskujący dostęp do usługi za pośrednictwem konta opiekuna nie może być stroną umowy z dostawcą. Dostawca stosuje środki w celu ustalenia, że opiekun umożliwiający dostęp zgodnie z ust. 1 jest podmiotem odpowiedzialności rodzicielskiej w odniesieniu do danego małoletniego, zgodnie z art. 26.

4. Projekt i sposób funkcjonowania dostępu kontrolowanego przez opiekuna, przyznanego na podstawie niniejszego artykułu, nie mogą w sposób nieproporcjonalny ograniczać prywatności małoletniego i wspierają jego autonomię i sprawczość, stosownie do rozwijających się zdolności małoletniego. Dostęp kontrolowany przez opiekuna, przyznany zgodnie z niniejszym artykułem, musi spełniać co najmniej następujące warunki:

a) domyślnie uruchamiane są narzędzia dla opiekunów określone w art. 20;

b) opiekun deklaruje wiek małoletniego, któremu umożliwia dostęp; taki dostęp nie jest umożliwiany w przypadku małoletniego w wieku poniżej 3 lat;

c) opiekun musi mieć możliwość ustalenia maksymalnego dziennego czasu trwania dostępu małoletniego, który nie może przekraczać jednej godziny;

d) opiekun musi mieć możliwość nadzorowania treści wyświetlanych lub rekomendowanych małoletniemu, z poszanowaniem prawa małoletniego do prywatności i z priorytetowym uwzględnieniem nadrzędnego interesu małoletniego;

e) opiekun ma możliwość zatwierdzania, ograniczania i usuwania wszelkich innych odbiorców usługi, z którymi małoletni może kontaktować się za pośrednictwem konta opiekuna;

f) opiekun ma możliwość zawieszenia dostępu małoletniego do konta w dowolnym momencie.

5. Dostęp kontrolowany przez opiekuna na podstawie niniejszego artykułu ustaje z chwilą osiągnięcia przez małoletniego wieku 13 lat, ustalonego na podstawie wieku zadeklarowanego zgodnie z ust. 4 lit. b) niniejszego artykułu. Pozostaje to bez uszczerbku dla możliwości utworzenia konta zgodnie z art. 5 ust. 2, jeżeli spełnione są warunki określone w tym artykule.

6. Komisja może przyjmować akty delegowane zgodnie z art. 40 w celu zmiany niniejszego rozporządzenia poprzez dostosowanie do postępu technologicznego i naukowego warunków określonych w ust. 1 i 4, w przypadku gdy takie zmiany

utrzymują poziom ochrony prywatności, bezpieczeństwa i ochrony małoletniego w internecie równoważny poziomowi zapewnianemu przez warunki określone w ust. 1 i 4 niniejszego artykułu.

ROZDZIAŁ III – UWZGLĘDNIANIE BEZPIECZEŃSTWA NA ETAPIE PROJEKTOWANIA

Sekcja I – Ogólny obowiązek uwzględniania bezpieczeństwa na etapie projektowania

Artykuł 8 – Ogólny obowiązek uwzględniania bezpieczeństwa na etapie projektowania

1. Dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI, ogólnych chatbotów konwersacyjnych oraz sklepów z aplikacjami, niezależnie od tego, czy te usługi lub systemy są dostępne za pośrednictwem konta, w tym usług i systemów dostępnych za pośrednictwem kont określonych w art. 5 ust. 3 i art. 6 ust. 3, zapewniają wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich. Dostawcy takich usług lub systemów domyślnie projektują te usługi i systemy zgodnie z wymogami określonymi w niniejszym rozdziale i stosują odstępstwo od tych wymogów wyłącznie po ustaleniu, że odbiorca usługi lub użytkownik systemu jest osobą dorosłą, przy wykorzystaniu potwierdzania wieku zgodnie z rozdziałem V.
2. Wypełnianie obowiązków określonych w niniejszym rozdziale pozostaje bez uszczerbku dla spoczywającego na dostawcach internetowych serwisów społecznościowych i usług platformy udostępniania wideo obowiązku odroczenia zakładania kont zgodnie z art. 6 oraz pozostaje bez uszczerbku dla spoczywającego na dostawcach usług platformy udostępniania wideo obowiązku dotyczącego, w stosownych przypadkach, kontrolowanego przez opiekuna dostępu małoletnich zgodnie z art. 7.
3. W przypadku gdy dostawcy internetowych serwisów społecznościowych lub usług platformy udostępniania wideo wdrażają towarzyszy AI lub ogólne chatboty konwersacyjne jako funkcjonalność w ramach świadczenia tych usług, do takich systemów AI mają zastosowanie wyłącznie obowiązki określone w sekcjach III, V i VI.

Sekcja II – Obowiązki dotyczące internetowych serwisów społecznościowych i usług platformy udostępniania wideo

Artykuł 9 – Uzależniające cechy projektowe

1. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo nie projektują, nie organizują ani nie świadczą swoich usług z zamiarem zachęcania, ani w sposób pozwalający racjonalnie przewidzieć, że zachęci małoletnich do kompulsywnego lub nadmiernego korzystania z internetowych serwisów społecznościowych i usług platformy udostępniania wideo.
2. Uznaje się, że kompulsywnemu lub nadmiernemu korzystaniu z usługi przez małoletnich w rozumieniu ust. 1 sprzyjają następujące funkcje:
   a) umożliwienie automatycznego odtwarzania treści i nieprzerwanego korzystania z treści bez skutecznych i regularnych przerw, które umożliwiają małoletnim zastanowienie nad chęcią do dalszego korzystania z treści;

b) kwestionowanie decyzji małoletniego o zaprzestaniu korzystania z usługi lub niezapewnianie małoletnim możliwości podjęcia takiej decyzji, na przykład ze względu na pojawiające się powiadomienia, które nie są wywołane interakcją małoletniego lub jego działaniem w ramach usługi ani nie są bezpośrednio związane z taką interakcją lub takim działaniem;

c) zachęcanie małoletnich do udostępniania treści lub angażowania się w transmisję treści w czasie rzeczywistym do nieokreślonej liczby odbiorców usługi lub nagradzanie za takie działania;

d) zachęcanie do zaangażowania w regularnych odstępach czasu lub z większą częstotliwością, w tym poprzez kary lub utratę korzyści za brak zaangażowania się regularnie lub w określonych odstępach czasu.

3. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo wprowadzają skuteczne środki w celu zapewnienia:

a) ograniczonego w czasie dostępu małoletnich do ich usług;

b) przerw w korzystaniu z ich usług przez małoletnich.

Środki takie opracowuje się w taki sposób, aby chronić czas nauki szkolnej i najważniejsze godziny snu małoletnich.

Artykuł 10 – Systemy rekomendacji

1. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo, którzy korzystają z systemów rekomendacji, projektują sugerowane przez nie informacje i optymalizują swoje systemy rekomendacji dla małoletnich w taki sposób, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich.

2. W celu wypełnienia obowiązków określonych w ust. 1 niniejszego artykułu dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo, którzy korzystają z systemów rekomendacji, optymalizują te systemy rekomendacji tak, aby nie wykorzystywały one podatności lub uwagi małoletniego oraz wprowadzają wskaźniki oceny uwzględniające wyniki w zakresie jakości, bezpieczeństwa i zdrowia psychicznego małoletnich, z zastosowaniem co najmniej następujących środków:

a) zapewnienie, aby systemy rekomendacji przy sugerowaniu informacji traktowały priorytetowo i kładły główny nacisk na wyraźne preferencje podane przez użytkownika;

b) domyślna dezaktywacja rekomendacji informacji sugerowanych przez system rekomendacji w oparciu o domyślne sygnały oparte na zaangażowaniu pochodzące z zachowania małoletnich w internecie;

c) zapewnienie, aby systemy rekomendacji nie polegały na gromadzeniu jakichkolwiek danych osobowych małoletnich pozyskanych spoza usługi;

d) zapewnienie, aby małoletni nie byli narażeni na informacje sugerowane przez systemy rekomendacji, które mogą stanowić zagrożenie dla ich prywatności, bezpieczeństwa i ochrony, również jeżeli stanowią takie zagrożenie w przypadku wielokrotnego wyświetlania.

3. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo, którzy korzystają z systemów rekomendacji, zapewniają i eksponują narzędzia, które pozwalają małoletnim:

a) modyfikować lub kontrolować parametry systemu rekomendacji, w tym poprzez łatwe usuwanie wszystkich wcześniej określonych preferencji;

b) wybierać co najmniej jedną opcję systemu rekomendacji, która nie jest oparta na profilowaniu w rozumieniu art. 4 pkt 4 rozporządzenia (UE) 2016/679.

Narzędzia, o których mowa w akapicie pierwszym, nie są projektowane w sposób zachęcający małoletnich do wyboru opcji opartej na profilowaniu, są oferowane podczas tworzenia konta i pozostają bezpośrednio dostępne z określonej sekcji interfejsu internetowego usługi, w której ustala się priorytetowo traktowane informacje, również dla odbiorców usługi nieposiadających konta.

Artykuł 11 – Bezpieczne ustawienia

1. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo wprowadzają środki zapewniające domyślne ustawienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich. Aby zapewnić zgodność z niniejszym ustępem, dostawcy ci domyślnie wyłączają co najmniej następujące ustawienia:

a) geolokalizacja i inne funkcje śledzenia;

b) dostęp do mikrofonu i kamery;

c) rekomendacje innych kont i synchronizacja kontaktów;

d) powiadomienia typu „push”, które w każdym przypadku powinny być zaprojektowane w sposób chroniący najważniejsze godziny snu i czas nauki szkolnej małoletnich.

2. Ustawienia domyślne, o których mowa w ust. 1, mogą zostać zmienione przez dostawcę wyłącznie w przypadku, gdy małoletni ukończył 15 lat oraz został w sposób jasny i jednoznaczny poinformowany o takich zmianach i jednoznacznie wyraził zgodę na takie zmiany. Ustawienia, o których mowa w ust. 1 lit. a), jeżeli zostały włączone przez małoletniego, wyłączają się po zakończeniu sesji w ramach usługi.

3. W przypadku gdy funkcje lub ustawienia stwarzają zagrożenie dla prywatności, bezpieczeństwa lub zdrowia małoletnich, dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo zapewniają, aby te funkcje lub ustawienia nie były dostępne dla małoletnich. Obejmuje to co najmniej funkcje sprzyjające porównaniom społecznym lub zmieniające wizerunek małoletniego, w szczególności poprzez jego nieproporcjonalne upiększanie lub idealizowanie.

Artykuł 12 – Zabezpieczenia dotyczące kontaktów i interakcji

1. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo wprowadzają środki zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w odniesieniu do kontaktów między małoletnimi a innymi odbiorcami usługi. Środki te gwarantują co najmniej, że:

a) inni odbiorcy usługi nie są w stanie nawiązać bezpośredniego kontaktu z małoletnim, jeżeli małoletni nie wyraził uprzednio zgody na taki kontakt;

b) małoletni posiadający konto nie są uwzględniani w rekomendacjach dotyczących kontaktów lub w podobnych funkcjach umożliwiających innym odbiorcom usługi, w tym małoletnim, rozszerzanie sieci kontaktów;

c) małoletni mogą być dodawani do grup o ograniczonej lub nieograniczonej liczbie odbiorców usługi wyłącznie za ich wyraźną zgodą;

d) małoletni mogą z łatwością zablokować każdego innego odbiorcę usługi bez ujawniania tożsamości zablokowanym odbiorcom usługi.

2. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo wdrażają zabezpieczenia uniemożliwiające odbiorcom ich usług stosowanie nakłaniania lub manipulacji wobec małoletnich, aby zgadzali się oni na bezpośredni kontakt, o którym mowa w ust. 1 lit. a).

3. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo wprowadzają środki ograniczające widoczność wszelkich informacji udostępnianych przez małoletnich oraz ich interakcji z innymi odbiorcami usługi. Środki te obejmują przynajmniej, co następuje:

a) inni odbiorcy usługi, którzy nie zostali wcześniej zaakceptowani przez małoletniego, domyślnie nie mają dostępu do informacji o koncie małoletniego ani do treści zamieszczanych lub udostępnianych przez małoletniego w ramach usługi;

b) odbiorcy usługi, którzy nie mają konta, nie mają dostępu do informacji o kontach małoletnich ani do treści zamieszczanych lub udostępnianych przez małoletnich w ramach usługi;

c) danych kontaktowych małoletnich, takich jak imię i nazwisko, numer telefonu, adres e-mail i adres zamieszkania, nie ujawnia się ani nie udostępnia innym odbiorcom usługi;

d) małoletni muszą mieć możliwość łatwego kontrolowania widoczności wszelkich udostępnianych treści, interakcji i powiązanych wskaźników w ramach usługi;

e) inni odbiorcy usługi nie mogą pobierać danych kontaktowych, informacji o lokalizacji lub koncie małoletnich ani żadnych treści zamieszczanych lub udostępnianych przez małoletnich w ramach usługi, ani robić zrzutów ekranu zawierających takie informacje;

f) małoletni domyślnie nie mogą prowadzić transmisji w czasie rzeczywistym treści tworzonych przez użytkowników, w tym poprzez transmisję strumieniową na żywo treści audiowizualnych.

Artykuł 13 – Bezpieczeństwo i ochrona transakcji gospodarczych

1. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo zapewniają, aby przed dokonaniem transakcji gospodarczej małoletni został poinformowany w jasny i łatwo zrozumiały sposób oraz w czasie rzeczywistym, że jest to transakcja gospodarcza. Przy zakupach dokonywanych w ramach usługi w walucie wirtualnej, którą można nabyć za pomocą środków pieniężnych w rozumieniu art. 4 pkt 25 dyrektywy (UE) 2015/2366, wyświetla się

odpowiednia wartość pieniężna w walucie urzędowej państwa członkowskiego, w którym odbiorca usługi ma miejsce zwykłego pobytu.

2. Dostawcy internetowych serwisów społecznościowych i usług platformy udostępniania wideo nie projektują, nie organizują, ani nie świadczą swoich usług w sposób, który może prowadzić do nadmiernych, impulsywnych lub niepożądanych wydatków. Obowiązek ten obejmuje nienarażanie małoletnich na zmienne mechanizmy nagradzające, w tym w przypadku gdy zakup odbywa się z wykorzystaniem walut wirtualnych, które można nabyć za pomocą środków pieniężnych w rozumieniu art. 4 pkt 25 dyrektywy (UE) 2015/2366.

Sekcja III – Obowiązki dotyczące towarzyszy AI i ogólnych chatbotów konwersacyjnych

Artykuł 14 – Obowiązki dotyczące towarzyszy AI i ogólnych chatbotów konwersacyjnych

1. Dostawcy towarzyszy AI i ogólnych chatbotów konwersacyjnych wprowadzają proporcjonalne i skuteczne środki w celu zapewnienia wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych oraz dobrostanu i rozwoju małoletnich, którzy mogą mieć dostęp do ich systemu AI. Środki te obejmują przynajmniej:

   a) zapewnienie, aby małoletni nie byli narażeni na uzależniające cechy projektowe, poprzez unikanie cech projektowych i zachowań systemowych symulujących relacje interpersonalne, które mogą powodować zależność emocjonalną, oraz poprzez stosowanie do takich systemów środków określonych w art. 9 ust. 1 i 3;

   b) zapewnienie małoletnim bezpiecznych ustawień poprzez zastosowanie do takich systemów środków określonych w art. 11, w tym poprzez zapewnienie, aby domyślnie w kolejnych interakcjach małoletniego z ich systemem nie wykorzystywano informacji ani analiz pochodzących z wcześniejszych interakcji, z wyjątkiem sytuacji, gdy jest to konieczne do ochrony bezpieczeństwa małoletniego, w celu zastosowania ustawień, o których mowa w art. 11;

   c) zapewnienie przejrzystości transakcji gospodarczych poprzez zastosowanie do takich systemów środków określonych w art. 13;

   d) zapewnienie, aby dostęp małoletnich w wieku poniżej 13 lat do usług, o których mowa w ust. 1, był możliwy i kontrolowany wyłącznie za pomocą narzędzi dla opiekunów, o których mowa w art. 20.

   e) przeprowadzanie najbardziej zaawansowanych ocen i testów systemu pod kątem zagrożeń dla zdrowia, bezpieczeństwa i praw podstawowych oraz dobrostanu fizycznego, psychicznego i emocjonalnego oraz rozwoju małoletnich, które mogą wystąpić, gdy małoletni wchodzą w interakcję z systemem, oraz wdrażanie odpowiednich zabezpieczeń w celu przeciwdziałania tym zagrożeniom przed wprowadzeniem systemu do obrotu lub oddaniem go do użytku;

   f) monitorowanie po wprowadzeniu do obrotu w celu identyfikacji, oceny i, w stosownych przypadkach, łagodzenia szkód i pojawiających się zagrożeń, o których mowa w lit. d) niniejszego ustępu, m.in. poprzez wykrywanie poważnych incydentów z udziałem małoletnich i reagowanie na nie, chyba że

dostawcą systemu jest mikroprzedsiębiorstwo lub małe przedsiębiorstwo w rozumieniu zalecenia 2003/361/WE.

2. W przypadku gdy towarzysz AI lub ogólny chatbot konwersacyjny jest wdrażany jako funkcjonalność internetowych serwisów społecznościowych, usług platformy udostępniania wideo lub gier internetowych w ramach świadczenia takich usług, dostawcy takich usług zapewniają, aby:

   a) towarzysz AI lub ogólny chatbot konwersacyjny nie był aktywowany automatycznie oraz aby funkcjonalność ta nie była wyświetlana w widocznym miejscu na interfejsie internetowym tej usługi;

   b) małoletni nie byli zachęcani do korzystania z towarzysza AI lub ogólnego chatbota konwersacyjnego;

   c) jeżeli jest to możliwe, małoletni mieli możliwość łatwej rezygnacji w dowolnym momencie z korzystania z towarzysza AI lub ogólnego chatbota konwersacyjnego.

3. Dostawcy towarzyszy AI i ogólnych chatbotów konwersacyjnych, którzy przestrzegają kodeksu postępowania uznanego przez Komisję za odpowiedni zgodnie z art. 23, mogą opierać się na tym kodeksie w celu wykazania zgodności z wymogami określonymi w niniejszym artykule.

Sekcja IV – Obowiązki dostawców gier internetowych

Artykuł 15 – Obowiązki dostawców gier internetowych

1. Dostawcy gier internetowych wprowadzają środki zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich. Środki te obejmują przynajmniej:

   a) zapewnienie, aby małoletni nie byli zachęcani do kompulsywnego lub nadmiernego korzystania z gry, poprzez stosowanie przepisów art. 9 ust. 1 oraz art. 9 ust. 2 lit. b) i d);

   b) zapewnienie, aby ustawienia dla małoletnich dawały wysoki poziom prywatności, bezpieczeństwa i ochrony, poprzez stosowanie przepisów art. 11 ust. 1;

   c) zapewnienie, aby kontakty między małoletnimi a innymi odbiorcami gry podlegały wysokiemu poziomowi prywatności, bezpieczeństwa i ochrony, poprzez stosowanie przepisów art. 12 ust. 1 i art. 12 ust. 3 lit. c);

   d) zapewnienie obowiązkowego dostępu do narzędzi dla opiekunów, o których mowa w art. 20, i zapewnienie, aby dostęp małoletnich w wieku poniżej 13 lat do usług, o których mowa w ust. 1, był możliwy i kontrolowany wyłącznie za pomocą narzędzi dla opiekunów, o których mowa w art. 20.

2. Dostawcy gier internetowych wprowadzają zabezpieczenia zapobiegające wykorzystywaniu gier do nakłaniania małoletnich do nawiązywania kontaktów w ramach innych usług, które mogą stanowić zagrożenie dla ich prywatności, bezpieczeństwa i ochrony.

3. W przypadku gdy dostawcy platform gier wideo zapewniają odbiorcom usługi możliwość tworzenia i zamieszczania gier wideo w ramach samej usługi, takie platformy gier wideo wprowadzają niezbędne oprogramowanie i środki

organizacyjne, aby umożliwić zgodność takich gier wideo z przepisami ust. 1 i 2 oraz art. 18 i art. 20.

4. Dostawcy gier internetowych, którzy przestrzegają kodeksu postępowania uznanego przez Komisję za odpowiedni zgodnie z art. 17, mogą opierać się na tym kodeksie w celu wykazania zgodności z wymogami określonymi w niniejszym artykule.

SEKCJA V – Obowiązki w zakresie dostępu dostosowanego do wieku

Artykuł 16 – Obowiązki dostawców sklepów z aplikacjami

1. Dostawcy sklepów z aplikacjami wprowadzają system klasyfikacji ze względu na wiek, aby umożliwić ustalenie, czy aplikacje rozpowszechniane za pośrednictwem ich usługi są dostosowane do wieku. Taki system klasyfikacji ze względu na wiek ma zastosowanie do każdego oprogramowania oferowanego w sklepie z aplikacjami i należycie uwzględnia rozwój zdolności umysłowych małoletnich.

2. Dostawcy sklepów z aplikacjami nie umożliwiają małoletnim dostępu do aplikacji, które są nieodpowiednie dla ich wieku zgodnie z systemem klasyfikacji ze względu na wiek wprowadzonym na podstawie ust. 1 niniejszego artykułu, ani zakupu takich aplikacji. Obowiązek ten nie ma wpływu na obowiązek dostawców usług oferowanych za pośrednictwem aplikacji objętych zakresem stosowania art. 6.

3. W przypadku gdy dostawca sklepu z aplikacjami dowie się, że za pośrednictwem jego usługi rozpowszechniane są aplikacje, które na mocy mającego zastosowanie prawa Unii lub prawa krajowego zgodnego z prawem Unii podlegają wyższemu minimalnemu wiekowi lub składają się głównie z treści podlegających wyższemu minimalnemu wiekowi niż wiek określony zgodnie z ust. 1, dostawca nie zezwala małoletnim poniżej tego wyższego minimalnego wieku z danego państwa członkowskiego lub danych państw członkowskich na dostęp do takich aplikacji ani na ich zakup.

4. W celu zapewnienia zgodności z ust. 2 i 3 dostawcy sklepów z aplikacjami oceniają wiek odbiorcy usługi zgodnie z rozdziałem V, w tym za pomocą narzędzi dla opiekunów, o których mowa w art. 20. Dostawcy sklepów z aplikacjami zapewniają, aby dostęp małoletnich w wieku poniżej 13 lat do usług, o których mowa w ust. 1, był możliwy i kontrolowany wyłącznie za pomocą narzędzi dla opiekunów, o których mowa w art. 20.

5. Dostawcy sklepów z aplikacjami podają do wiadomości publicznej informacje opisujące w jasny i przystępny sposób metodykę, kryteria i źródła wykorzystywane w ich systemach klasyfikacji ze względu na wiek.

6. Dostawcy sklepów z aplikacjami umożliwiają oferowanie w swoich sklepach unijnego rozwiązania z zakresu weryfikacji wieku wykorzystującego unijne poświadczenie dowodu wieku, certyfikowanego jako zgodne z unijnym systemem weryfikacji wieku i ujętego w odpowiednich wykazach UE, o których mowa w art. 30 ust. 1.

Artykuł 17 – Kodeksy postępowania dotyczące klasyfikacji ze względu na wiek oraz gier internetowych

1. Komisja wspiera i ułatwia opracowywanie kodeksów postępowania na szczeblu Unii do dnia [ten sam dzień i miesiąc co data rozpoczęcia stosowania plus jeden rok] r. z udziałem dostawców sklepów z aplikacjami i gier internetowych, twórców

i dostawców treści cyfrowych, w tym aplikacji i gier internetowych, dostawców systemów klasyfikacji ze względu na wiek, organizacji reprezentujących małoletnich i ich opiekunów, organizacji społeczeństwa obywatelskiego specjalizujących się w ochronie małoletnich w internecie, a także odpowiednich organów. Kodeksy postępowania muszą przyczyniać się do zharmonizowanego ustanowienia i stosowania systemów klasyfikacji ze względu na wiek, w tym systemów, o których mowa w art. 16 ust. 1, w szczególności poprzez określenie wspólnych kryteriów i metod na potrzeby takich systemów, oraz do skutecznego stosowania art. 15 w odniesieniu do gier internetowych.

2. Komisja stara się zapewnić, aby w kodeksach postępowania uwzględniono co najmniej:

a) dążenie do jasno określonego i jednoznacznego celu, jakim jest umożliwienie i ułatwienie wzajemnego uznawania i spójnego stosowania klasyfikacji ze względu na wiek przez dostawców sklepów z aplikacjami i gier internetowych we wszystkich państwach członkowskich;

b) określenie odpowiednich kryteriów, metod i źródeł informacji na potrzeby oceny dostosowania treści do wieku, w szczególności w odniesieniu do treści zawierających przemoc, treści o charakterze seksualnym, treści związanych z hazardem i treści dotyczących samookaleczania, a także do zakupów wewnątrz aplikacji, ryzyka kontaktu i uzależniających cech projektowych;

c) ustanowienie bezpłatnych środków ochrony prawnej i mechanizmów dochodzenia roszczeń dla dostawców treści, w tym twórców aplikacji, na potrzeby rozstrzygania sporów związanych z klasyfikacją dostarczanych treści ze względu na wiek przez organ, który jest bezstronny i niezależny, w tym niezależny finansowo, od dostawców i odbiorców usługi;

d) zapewnienie zharmonizowanych, łatwo rozpoznawalnych i zrozumiałych oznaczeń klasyfikacji ze względu na wiek i deskryptorów tekstowych, które będą wyświetlane w widocznym miejscu i przed uzyskaniem dostępu do treści lub ich zakupem;

e) zapewnienie regularnego, przejrzystego i niezależnego monitorowania i oceny realizacji celów, w tym poprzez uwzględnienie kluczowych wskaźników skuteczności działania służących do pomiaru realizacji ich celów oraz regularne aktualizacje odzwierciedlające rozwój technologiczny i pojawiające się zagrożenia dla małoletnich;

f) określenie, w odniesieniu do gier internetowych, odpowiednich środków i metod na potrzeby wypełniania obowiązków określonych w art. 15 ust. 1, 2, 3 i 4, opartych, w stosownych przypadkach, na istniejących ogólnoeuropejskich ramach klasyfikacji ze względu na wiek, w tym na ich kryteriach dotyczących funkcji interaktywnych i praktyk monetyzacji, oraz zapewnienie regularnej aktualizacji tych środków i metod w świetle rozwoju naukowego i technologicznego oraz pojawiających się zagrożeń dla małoletnich.

3. Do dnia [ten sam dzień co data wejścia w życie plus 42 miesiące] r. Komisja ocenia, czy kodeksy postępowania spełniają cele określone w ust. 2 i są odpowiednie na potrzeby wykazania zgodności z odpowiednimi obowiązkami. Komisja regularnie monitoruje i ocenia realizację ich celów, z uwzględnieniem kluczowych wskaźników skuteczności działania, które mogą one zawierać, oraz publikuje swoją ocenę.

W przypadku gdy Komisja ocenia przestrzeganie ust. 2 lit. f), zastosowanie ma art. 15 ust. 4.

SEKCJA VI – Ogólne obowiązki dotyczące sprawczości małoletnich i narzędzia zwiększające podmiotowość małoletnich i opiekunów

Artykuł 18 – Sprawczość małoletnich

1. Dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI i ogólnych chatbotów konwersacyjnych zapewniają, aby funkcje, komunikacja, informacje, narzędzia i mechanizmy usługi i systemu dające kontrolę użytkownikowi, ostrzeżenia i wszelkie inne informacje, o których mowa w rozdziale III, były łatwo dostępne dla wszystkich małoletnich i przedstawione w sposób dla nich zrozumiały. W przypadku gdy dostawca jest dostawcą bardzo dużej platformy internetowej wskazanej zgodnie z art. 33 rozporządzenia (UE) 2022/2065, dostawca ten zapewnia, aby informacje, o których mowa w niniejszym ustępie, były udostępniane w języku urzędowym państwa członkowskiego lub językach urzędowych państw członkowskich, w których świadczona jest usługa.

2. Dostawcy, o których mowa w ust. 1, wprowadzają, co następuje:

   a) narzędzia, które umożliwiają małoletnim kontrolowanie i przekazywanie informacji zwrotnych na temat treści, promptów, sugerowanych informacji i wyników wyszukiwania, z którymi mają styczność, oraz które mają natychmiastowy i trwały wpływ na takie treści, wezwania do działania, sugerowane informacje i wyniki wyszukiwania;

   b) mechanizmy umożliwiające małoletnim kontrolowanie ustawień, które określają sposób ich interakcji i komunikacji z usługą lub systemem, a także sposób przekazywania, tworzenia lub generowania treści w ramach usługi lub systemu, w tym sygnały ostrzegawcze, oraz wyjaśnienia, które umożliwiają tymczasowe zmiany i zapewniają małoletnim możliwość łatwego powrotu do poprzednich lub domyślnych ustawień.

Artykuł 19 – Przyjazne dziecku narzędzia zgłaszania i wsparcia dla małoletnich

1. Dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, platform gier wideo, towarzyszy AI i ogólnych chatbotów konwersacyjnych wprowadzają mechanizmy umożliwiające małoletnim zgłaszanie odpowiednio treści, kont, grup, funkcji lub zachowań, które uznają za szkodliwe dla swojej prywatności, bezpieczeństwa lub ochrony. Takie mechanizmy muszą być łatwo dostępne i zaprojektowane w sposób zrozumiały dla małoletnich. W przypadku gdy dostawca jest dostawcą bardzo dużej platformy internetowej wskazanej zgodnie z art. 33 rozporządzenia (UE) 2022/2065, dostawca ten zapewnia, aby mechanizmy te były udostępniane w języku urzędowym państwa członkowskiego lub językach urzędowych państw członkowskich, w których świadczona jest usługa.

2. W przypadku gdy dostawca, o którym mowa w ust. 1, jest platformą internetową podlegającą art. 17 rozporządzenia (UE) 2022/2065, wszelkie ograniczenia nałożone w następstwie zgłoszeń, o których mowa w ust. 1 niniejszego artykułu, uznaje się za ograniczenie w zakresie widoczności zgodnie z art. 17 ust. 1 lit. a) rozporządzenia (UE) 2022/2065.

3. Dostawcy, o których mowa w ust. 1, wprowadzają niezbędne środki techniczne i organizacyjne w celu zapewnienia, aby zgłoszenia dokonywane przez małoletnich zgodnie z ust. 1 były przetwarzane i rozpatrywane priorytetowo i bez zbędnej zwłoki oraz aby małoletni otrzymywali informacje na temat wszczętej procedury i możliwości dochodzenia roszczeń.

4. Dostawcy, o których mowa w ust. 1, są zobowiązani do:

   a) zapewniania małoletnim dostępu do wsparcia i wiarygodnych źródeł informacji w przypadku napotkania w ramach usługi lub systemu nielegalnych lub szkodliwych treści, w tym poprzez informowanie małoletnich o dostępnych zasobach i organizacjach na szczeblu krajowym i unijnym;

   b) zapewniania, aby wsparcie i wiarygodne źródła informacji, o których mowa w lit. a) niniejszego ustępu, były przedstawiane małoletnim w razie potrzeby, a co najmniej po dokonaniu przez nich zgłoszenia zgodnie z ust. 1;

   c) podejmowania racjonalnych starań w celu wyświetlania jasnych komunikatów ostrzegawczych tam, gdzie małoletni prawdopodobnie będą publikować treści lub będą narażeni na treści lub interakcje stwarzające zagrożenie dla ich prywatności, bezpieczeństwa lub ochrony.

Artykuł 20 – Narzędzia dla opiekunów

1. Dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI i ogólnych chatbotów konwersacyjnych wdrażają skuteczne, przystępne i przyjazne dla użytkownika narzędzia dla opiekunów, które spełniają co najmniej następujące warunki:

   a) są dostosowane do wieku małoletniego i należycie uwzględniają stopniowy rozwój małoletniego;

   b) są łatwe w użyciu, łatwo dostępne i łatwe do aktywowania dla małoletnich i opiekunów;

   c) zapewniają, aby zmiany można było wprowadzać wyłącznie przy takim samym poziomie upoważnienia, jaki jest wymagany przy początkowej aktywacji narzędzi;

   d) są skuteczne i nie można ich łatwo obejść ani pozbawić skuteczności przez sposób zaprojektowania lub funkcjonowania usługi lub systemu;

   e) nie ograniczają w sposób nieproporcjonalny praw małoletnich;

   f) nie naruszają sprawczości i prywatności małoletniego.

2. Dostawcy, o których mowa w ust. 1, zapewniają, aby małoletni byli informowani o każdym przypadku korzystania z narzędzia dla opiekunów, o którym mowa w ust. 1.

3. Dostawcy, o których mowa w ust. 1, zachęcają opiekunów do korzystania z narzędzi, o których mowa w tym ustępie, i regularnie przypominają im o ich dostępności i celach oraz o potrzebie ich aktualizacji. Obejmuje to wyświetlanie jasnych komunikatów ostrzegawczych dotyczących zarządzania ustawieniami w odniesieniu do małoletnich.

4. Dostawcy, o których mowa w ust. 1, włączają następujące mechanizmy do narzędzi dla opiekunów, o których mowa w tym ustępie:

a) skuteczne środki zapewniające dostęp ograniczony w czasie zgodnie z art. 9 ust. 3, art. 14 ust. 1 lit. b) i art. 15 ust. 1 lit. b);

b) mechanizmy służące do zarządzania ustawieniami zgodnie z art. 11 i 12;

c) mechanizmy umożliwiające opiekunom, w imieniu małoletnich, zgłaszanie treści, kont, grup lub zachowań, które uważają oni za szkodliwe dla prywatności, bezpieczeństwa lub ochrony małoletnich zgodnie z art. 19 ust. 1.

5. Dostawcy bardzo dużych platform internetowych wskazanych zgodnie z art. 33 rozporządzenia (UE) 2022/2065 zapewniają interoperacyjność narzędzi dla opiekunów, o których mowa w ust. 1, z narzędziami dla opiekunów udostępnianymi przez osoby trzecie, w stosownych przypadkach zgodnie z warunkami określonymi w art. 6 rozporządzenia (UE) 2022/1925.

6. Dostawcy, o których mowa w ust. 1, zapewniają opiekunom i małoletnim możliwość zgłaszania zgodnie z art. 19 przypadków, w których narzędzia dla opiekunów, o których mowa w ust. 1, nie działają i nie funkcjonują zgodnie z przepisami.

7. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 40 w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie wymogów technicznych i operacyjnych dotyczących narzędzi dla opiekunów, o których mowa w ust. 1 niniejszego artykułu.

Artykuł 21 – Skargi zbiorowe

1. Bez uszczerbku dla art. 86 rozporządzenia (UE) 2022/2065 i dyrektywy (UE) 2020/1828 lub dla jakiegokolwiek innego rodzaju przepisów dotyczących przedstawicielstwa na mocy prawa krajowego małoletni i opiekunowie będący odbiorcami internetowych serwisów społecznościowych, usług platformy udostępniania wideo, platform gier wideo oraz użytkownikami towarzyszy AI lub ogólnych chatbotów konwersacyjnych mają co najmniej prawo umocować podmiot, organizację lub zrzeszenie do wykonania w imieniu małoletnich praw przyznanych niniejszym rozporządzeniem, pod warunkiem że taki podmiot, taka organizacja lub takie zrzeszenie spełniają wszystkie następujące warunki:

a) prowadzą działalność nienastawioną na zysk;

b) zostały należycie ustanowione zgodnie z prawem państwa członkowskiego;

c) ich cele statutowe obejmują prawnie uzasadniony interes polegający na zapewnieniu przestrzegania niniejszego rozporządzenia.

2. Oprócz prawa do wniesienia skargi zgodnie z art. 53 rozporządzenia (UE) 2022/2065 małoletni i opiekunowie, którzy są odbiorcami internetowych serwisów społecznościowych, usług platformy udostępniania wideo, platform gier wideo oraz użytkownikami towarzyszy AI i ogólnych chatbotów konwersacyjnych, a także każdy podmiot, organizacja lub zrzeszenie, o których mowa w ust. 1 niniejszego artykułu, mają prawo wnieść skargę w związku z zarzucanym naruszeniem niniejszego rozporządzenia przeciwko dostawcom wyżej wymienionych usług i systemów do właściwego organu określonego zgodnie z art. 34 w państwie członkowskim, w którym znajduje się lub ma siedzibę odbiorca usługi lub użytkownik systemu, lub do Europejskiego Urzędu ds. Sztucznej Inteligencji w odniesieniu do towarzyszy AI lub ogólnych chatbotów konwersacyjnych objętych jego wyłączną kompetencją na podstawie art. 75 ust. 1 rozporządzenia (UE) 2024/1689.

SEKCJA VII – Inne obowiązki w zakresie należytej staranności na rzecz bezpiecznego środowiska internetowego

Artykuł 22 – Obowiązek monitorowania spoczywający na dostawcach bardzo dużych platform internetowych

1. Dostawcy usług, o których mowa w art. 8 ust. 1 niniejszego rozporządzenia, które zostały wskazane jako bardzo duże platformy internetowe zgodnie z art. 33 rozporządzenia (UE) 2022/2065, monitorują, testują i oceniają skuteczność środków wdrożonych zgodnie z niniejszym rozdziałem.

2. Ocena, o której mowa w ust. 1 niniejszego artykułu, stanowi część oceny ryzyka przeprowadzanej na podstawie art. 34 rozporządzenia (UE) 2022/2065.

Artykuł 23 – Kodeksy postępowania

1. Komisja wspiera i ułatwia opracowywanie dobrowolnych kodeksów postępowania na szczeblu Unii, aby przyczynić się do właściwego stosowania niniejszego rozporządzenia. Komisja zaprasza dostawców odpowiednich usług i systemów objętych zakresem stosowania niniejszego rozporządzenia, odpowiednie właściwe organy krajowe, organizacje społeczeństwa obywatelskiego, przemysł, środowisko akademickie, rodziców, wychowawców i inne odpowiednie zainteresowane strony do udziału w opracowywaniu tych kodeksów postępowania.

2. Nadając skuteczność przepisom ust. 1, Komisja dąży do zapewnienia, aby kodeksy postępowania jasno określały swoje cele szczegółowe, zawierały zobowiązania do wprowadzenia konkretnych środków służących osiągnięciu tych celów, a także należycie uwzględniały specyfikę różnych dostarczanych usług i systemów oraz potrzeby i interesy wszystkich zainteresowanych stron, w szczególności małoletnich, na szczeblu Unii. Komisja dąży również do zapewnienia, aby uczestnicy regularnie składali sprawozdania Komisji i swoim odpowiednim właściwym organom na podstawie niniejszego rozporządzenia. W zobowiązaniach w zakresie sprawozdawczości, których podjęcia oczekuje Komisja, uwzględnia się różnice między poszczególnymi dostawcami pod względem wielkości i zdolności.

3. Po konsultacji z Europejską Radą ds. Usług Cyfrowych lub Europejską Radą ds. Sztucznej Inteligencji w odniesieniu do aspektów kodeksów, które wchodzą w zakres ich kompetencji, Komisja ocenia, czy kodeksy postępowania spełniają cele określone w ust. 1 i 3 i są odpowiednie do wykazania zgodności z odpowiednimi obowiązkami określonymi w niniejszym rozporządzeniu. Komisja publikuje tę ocenę. Komisja regularnie monitoruje i ocenia osiągnięcie celów kodeksów postępowania oraz, po konsultacji z Europejską Radą ds. Usług Cyfrowych lub Europejską Radą ds. Sztucznej Inteligencji, w stosownych przypadkach aktualizuje ocenę.

4. Komisja wspiera i ułatwia regularne przeglądy i dostosowania kodeksów postępowania.

5. Komisja zachęca również do opracowywania najlepszych praktyk w każdej dziedzinie objętej zakresem stosowania niniejszego rozporządzenia. Może to dotyczyć takich obszarów jak badania w trakcie opracowywania produktów lub normy kontroli. Pozostaje to bez uszczerbku dla art. 5.

Art. 24 – Przedstawiciele prawni

1. Dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI i ogólnych chatbotów konwersacyjnych, którzy nie mają siedziby w Unii, ale oferują usługi lub systemy w Unii, wyznaczają na piśmie osobę prawną lub fizyczną do działania w charakterze ich przedstawiciela prawnego w jednym z państw członkowskich, w których dostawca oferuje swoje usługi lub system. Jeżeli jednak tacy dostawcy wyznaczyli już przedstawiciela prawnego na podstawie art. 13 rozporządzenia (UE) 2022/2065 lub na podstawie art. 22 lub 54 rozporządzenia (UE) 2024/1689, mogą rozszerzyć mandat tej osoby prawnej lub fizycznej na wszystkie kwestie niezbędne do otrzymywania, przestrzegania i egzekwowania decyzji wydanych w związku z niniejszym rozporządzeniem.

2. Zastosowanie ma art. 13 ust. 2–5 rozporządzenia (UE) 2022/2065, a odesłania do rozporządzenia (UE) 2022/2065 odczytuje się jako odesłania do niniejszego rozporządzenia w odniesieniu do obowiązków określonych w niniejszym rozporządzeniu dotyczących dostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo i gier internetowych. Zastosowanie ma art. 22 ust. 2, 3 i 4 rozporządzenia (UE) 2024/1689 lub art. 54 ust. 2–5 tego rozporządzenia, a odesłania do obowiązków określonych w rozporządzeniu (UE) 2024/1689 odczytuje się jako odesłania do niniejszego rozporządzenia w odniesieniu do obowiązków określonych w niniejszym rozporządzeniu dotyczących dostawców towarzyszy AI i ogólnych chatbotów konwersacyjnych.

Artykuł 25 – Zmiany wymienionych środków

1. Komisja może przyjmować akty delegowane zgodnie z art. 40 w celu zmiany art. 9 ust. 2, art. 10 ust. 2, art. 11 ust. 1, art. 12 ust. 1, art. 12 ust. 2, art. 14 ust. 1, art. 15 ust. 1 i art. 18 ust. 2 w odniesieniu do dostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych, towarzyszy AI i ogólnych chatbotów konwersacyjnych, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w ramach ich usługi lub systemu. Te akty delegowane muszą opierać się na zidentyfikowanych pojawiających się zagrożeniach dla zdrowia i dobrostanu, a także prywatności, bezpieczeństwa i ochrony małoletnich, sprawiając, że konieczna staje się aktualizacja następujących obowiązków w celu zapewnienia skutecznego ich wypełniania:

   a) zakazy praktyk mających na celu zachęcanie lub w przypadku których można racjonalnie przewidzieć, że będą zachęcały małoletnich do kompulsywnego lub nadmiernego korzystania z usługi, o czym mowa w art. 9 ust. 2;

   b) środki zapewniające, aby systemy rekomendacji były projektowane w sposób zapewniający wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, o czym mowa w art. 10 ust. 2;

   c) domyślne ustawienia zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony kont małoletnich, o czym mowa w art. 11 ust. 1;

   d) środki zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w odniesieniu do kontaktów między małoletnimi a innymi odbiorcami usługi, o czym mowa w art. 12 ust. 1, oraz środki ograniczające

widoczność wszelkich informacji udostępnianych przez małoletnich oraz ich interakcji z innymi odbiorcami usługi, o czym mowa w art. 12 ust. 2;

e) środki zapewniające wysoki poziom ochrony zdrowia, bezpieczeństwa, praw podstawowych i dobrostanu małoletnich, którzy mogą mieć dostęp do towarzyszy AI i ogólnych chatbotów konwersacyjnych, o czym mowa w art. 14 ust. 1;

f) środki zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w grach internetowych, o czym mowa w art. 15 ust. 1;

g) środki zapewniające sprawczość małoletnich, o czym mowa w art. 18 ust. 2.

2. Rozważając przyjęcie aktu delegowanego, Komisja musi brać pod uwagę:

a) zakres, w jakim dane zagrożenie już wyrządziło szkodę dla zdrowia i dobrostanu lub miało niepożądany wpływ na prywatność, bezpieczeństwo i ochronę lub prawa podstawowe małoletnich lub wzbudziło istotne obawy co do prawdopodobieństwa wystąpienia takiej szkody lub niepożądanego wpływu, czego potwierdzeniem są na przykład zgłoszenia lub udokumentowane zarzuty przedstawione właściwym organom krajowym lub, w stosownych przypadkach, inne zgłoszenia;

b) potencjalny zakres takiej szkody lub takiego niepożądanego wpływu, w szczególności pod względem ich nasilenia i możliwości oddziaływania na wiele osób lub nieproporcjonalnego oddziaływania na określoną grupę lub osoby;

c) wpływ istniejących środków na przeciwdziałanie takim zagrożeniom, w tym zamierzony cel takich środków, zakres, w jakim środki te są lub mogą być stosowane, oraz skuteczność takich środków w odniesieniu do zdrowia, dobrostanu oraz prywatności, bezpieczeństwa i ochrony małoletnich.

ROZDZIAŁ IV – WERYFIKACJA ODPOWIEDZIALNOŚCI RODZICIELSKIEJ

Artykuł 26 – Weryfikacja odpowiedzialności rodzicielskiej

1. W celu utworzenia konta o ograniczonych funkcjach zgodnie z art. 6 ust. 2 lub o dostosowanym do wieku doświadczeniu na platformach udostępniania wideo zgodnie z art. 7 ust. 2 oraz w celu wdrożenia skutecznych, dostępnych i przyjaznych dla użytkownika narzędzi dla opiekunów zgodnie z art. 20 ust. 1 dostawca usługi, o której mowa w tych przepisach, musi mieć możliwość:

a) wykorzystywania sygnałów odpowiedzialności rodzicielskiej w oparciu o ogólnodostępne oficjalne internetowe bazy danych lub interfejsy internetowe udostępniane przez państwo członkowskie;

b) wykorzystywania sygnałów odpowiedzialności rodzicielskiej, które dostawca usług może już posiadać w związku z wcześniejszymi interakcjami z daną usługą danego małoletniego i danej osoby dorosłej posiadającej odpowiedzialność rodzicielską;

c) przyjmowania oświadczenia własnego osoby dorosłej, na której spoczywa odpowiedzialność rodzicielska, co najmniej do czasu przyjęcia aktu delegowanego, o którym mowa w ust. 3.

2. Wykorzystując sygnały, o których mowa w ust. 1 lit. a), dostawca podejmuje rozsądne starania w celu zweryfikowania, czy dostępne informacje są wiarygodne i kompletne.

3. Wykorzystując oświadczenia własne, o których mowa w ust. 1 lit. c), dostawca podejmuje rozsądne starania w celu zweryfikowania, czy osoba dorosła składająca oświadczenie własne wykonuje odpowiedzialność rodzicielską.

4. Weryfikację odpowiedzialności rodzicielskiej na podstawie ust. 1 przeprowadza się w sposób chroniący prywatność i nie może ona prowadzić do dodatkowego przetwarzania danych osobowych, które mogłoby umożliwić dostawcy usługi ustalenie lokalizacji danej osoby dorosłej lub danego małoletniego czy też śledzenie, targetowanie lub profilowanie danej osoby dorosłej lub danego małoletniego.

5. Komisja jest uprawniona do przyjęcia aktu delegowanego zgodnie z art. 39 w celu uzupełnienia niniejszego rozporządzenia przez określenie sygnałów wskazujących na odpowiedzialność rodzicielską zgodnie z ust. 1 lit. a) niniejszego artykułu.

ROZDZIAŁ V – POTWIERDZANIE WIEKU

Sekcja I – Ogólne zasady potwierdzania wieku

Artykuł 27 – Ogólne zasady potwierdzania wieku

Gdy dostawcy usług i systemów podlegających rozdziałom II i III wdrażają rozwiązania w zakresie potwierdzania wieku w celu wypełnienia swoich obowiązków określonych w niniejszym rozporządzeniu, zapewniają oni, aby rozwiązania te zapewniały wysoki poziom dokładności, wiarygodności, bezpieczeństwa, solidności, nieinwazyjności, ochrony prywatności, ochrony danych oraz niedyskryminacji.

Artykuł 28 – Ochrona danych w odniesieniu do potwierdzania wieku

1. Rozwiązania w zakresie potwierdzania wieku nie mogą umożliwiać identyfikacji odbiorcy ani lokalizowania, śledzenia, targetowania, profilowania lub wysyłania reklam do odbiorców w żadnym celu.

2. Dostawcy usług i systemów objętych zakresem stosowania niniejszego rozporządzenia oraz wszelkie podmioty prowadzące działania w celu potwierdzania wieku w imieniu takich dostawców lub wraz z nimi nie przechowują, nie pozyskują ani nie przetwarzają większej ilości danych osobowych niż jest to absolutnie niezbędne do oceny, czy odbiorca usługi lub użytkownik systemu osiągnął progi wiekowe określone w niniejszym rozporządzeniu, oraz nie przetwarzają dalej, nie udostępniają ani nie łączą tych informacji z żadnymi dodatkowymi danymi, bez uszczerbku dla art. 29 ust. 6, i nie łączą danych osobowych przechowywanych lub związanych z korzystaniem z systemu z danymi osobowymi pochodzącymi z jakichkolwiek innych usług oferowanych przez dostawcę lub świadczonych przez osoby trzecie.

3. Dostawcy usług i systemów objętych zakresem stosowania niniejszego rozporządzenia oraz wszelkie podmioty prowadzące działania w celu potwierdzania wieku w imieniu takich dostawców lub wraz z nimi zapewniają, aby stosowane

środki opierały się na najnowocześniejszej technologii. Każdy środek potwierdzania wieku musi być dowodem z wiedzą zerową.

4. Na zasadzie odstępstwa od ust. 2 dostawcy, o których mowa w art. 16 ust. 4 i art. 8 ust. 1, mogą przechowywać, na poziomie konta i wyłącznie w celu uniknięcia wielokrotnego potwierdzania wieku, sygnał wieku potwierdzający, że użytkownik osiągnął konkretny próg wieku na podstawie niniejszego rozporządzenia. Taki sygnał wieku musi ograniczać się do minimum informacji niezbędnych do tego celu.

5. Dostawcy usług i systemów objętych zakresem stosowania niniejszego rozporządzenia wprowadzają niezbędne środki techniczne i organizacyjne w celu zapewnienia zgodności z ust. 1, 2, 3 i 4.

Sekcja II – Szczegółowe obowiązki w zakresie potwierdzania wieku

Artykuł 29 – Rozwiązania w zakresie potwierdzania wieku

1. Dostawcy usług, o których mowa w art. 6 niniejszego rozporządzenia, wprowadzają rozwiązania z zakresu weryfikacji wieku na potrzeby sprawdzania, na warunkach określonych w niniejszym rozdziale, czy odbiorca usługi osiągnął minimalny wiek na podstawie tych przepisów lub, w stosownych przypadkach, czy konieczne jest utworzenie konta rodzicielskiego.

2. Do celów zgodności z art. 6 dostawcy, o których mowa w tym ustępie, opierają się wyłącznie na unijnym rozwiązaniu z zakresu weryfikacji wieku wykorzystującym unijne poświadczenie dowodu wieku, które jest dostarczane przez osobę trzecią, certyfikowane jako zgodne z unijnym systemem weryfikacji wieku i ujęte w odpowiednich unijnych listach, o których mowa w art. 30 ust. 1 lit. a) i b), lub możliwe do zweryfikowania na podstawie tych wykazów.

3. Unijne rozwiązania z zakresu weryfikacji wieku i unijne poświadczenia dowodu wieku muszą być certyfikowane przez organ publiczny jako zgodne z wymogami unijnego systemu weryfikacji wieku określonymi zgodnie z art. 30 ust. 2. Europejskie portfele tożsamości cyfrowej certyfikowane zgodnie z art. 5c rozporządzenia (UE) nr 910/2014, które spełniają wymogi unijnego systemu weryfikacji wieku, uznaje się za certyfikowane zgodnie z niniejszym ustępem. Dostawcy unijnych poświadczeń dowodu wieku i dostawcy unijnych rozwiązań z zakresu weryfikacji wieku muszą spełniać wymogi unijnego systemu weryfikacji wieku.

4. Na potrzeby wypełniania obowiązków określonych w art. 8 ust. 1, art. 16 ust. 2 i art. 16 ust. 3 dostawcy, których to dotyczy, mogą stosować rozwiązania w zakresie potwierdzania wieku inne niż unijne rozwiązania z zakresu weryfikacji wieku, o których mowa w ust. 2, jeżeli są w stanie wykazać, że rozwiązania te spełniają wymogi określone w art. 27 i 28.

5. Dostawcy usług i systemów, o których mowa w ust. 1 i 4, zapewniają odbiorcom dostęp do skutecznego wewnętrznego mechanizmu rozpatrywania skarg umożliwiającego im składanie, drogą elektroniczną i nieodpłatnie, skarg w odniesieniu do wyniku potwierdzania wieku, o którym mowa w tych ustępach, w przypadku gdy odbiorca uzna wynik potwierdzania wieku za nieprawidłowy. Dostawcy platform internetowych, zgodnie z definicją w art. 3 lit. i) rozporządzenia 2022/2065, mogą, na potrzeby zapewniania zgodności z niniejszym artykułem,

korzystać z mechanizmu rozpatrywania skarg określonego w art. 20 rozporządzenia 2022/2065.

6. W przypadku gdy dostawca systemu operacyjnego otrzymał sygnał wieku użytkownika i gdy potwierdzenie wieku wykorzystane do uzyskania tego sygnału wieku jest zgodne z wymogami określonymi na podstawie art. 27, po uzyskaniu zgody użytkownika dostawca systemu operacyjnego umożliwia udostępnianie sygnału wieku dostawcom objętym zakresem niniejszego rozporządzenia, gdy taki sygnał wieku użytkownika jest wymagany do zapewnienia zgodności z niniejszym rozporządzeniem.

Artykuł 30 – Uprawnienia Komisji

1. Komisja prowadzi:

   a) unijną listę dostawców unijnych poświadczeń dowodu wieku certyfikowanych zgodnie z art. 29 ust. 2 i notyfikowanych przez dowolne państwo członkowskie;

   b) unijną listę unijnych rozwiązań z zakresu weryfikacji wieku certyfikowanych zgodnie z art. 29 ust. 2 i notyfikowanych przez dowolne państwo członkowskie.

   Komisja publikuje i aktualizuje unijną listę oraz utrzymuje ją w formacie bezpiecznym i nadającym się do odczytu maszynowego.

2. Komisja przyjmuje akty wykonawcze określające specyfikacje stanowiące podstawę funkcjonowania unijnego systemu weryfikacji wieku, w tym wymogi mające zastosowanie do unijnych rozwiązań z zakresu weryfikacji wieku oraz do wydawania, prezentowania i weryfikacji unijnych poświadczeń dowodu wieku. Takie akty wykonawcze muszą ograniczać się do tego, co jest konieczne do zapewnienia skutecznego, bezpiecznego, chroniącego prywatność, interoperacyjnego i jednolitego wdrożenia art. 29 ust. 2 i 3, i opierać się na zasadzie minimalizacji danych, ograniczenia celu, bezpieczeństwa, neutralności technologicznej i proporcjonalności, a także muszą zapewniać interoperacyjność z europejskimi portfelami tożsamości cyfrowej zapewnianymi na podstawie art. 5a rozporządzenia (UE) nr 910/2014. W aktach wykonawczych określa się szczegółowe wymogi techniczne, organizacyjne, dotyczące prywatności i bezpieczeństwa mające zastosowanie do unijnych poświadczeń dowodu wieku i ich dostawców oraz do unijnych rozwiązań z zakresu weryfikacji wieku i ich dostawców, dowody i procedury wykazywania i oceny organów publicznych oraz specyfikacje unijnych list, o których mowa w ust. 1. Akty wykonawcze mogą również zawierać wymogi dotyczące znaku zaufania dla rozwiązań z zakresu weryfikacji wieku. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 40 ust. 2.

3. Komisja przyjmuje akty delegowane, zgodnie z art. 39, w celu uzupełnienia niniejszego rozporządzenia poprzez określenie:

   a) wymogów mających zastosowanie do alternatywnych rozwiązań w zakresie potwierdzania wieku, o których mowa w art. 29 ust. 4, w tym wymogów niezbędnych do wykazywania zgodności z art. 27 i 28. Te akty delegowane określają szczegółowe mające zastosowanie wymogi techniczne, organizacyjne, dotyczące prywatności i bezpieczeństwa;

b) obowiązków mających zastosowanie do systemów operacyjnych, o których mowa w art. 29 ust. 6, w tym wymogów niezbędnych do zapewniania bezpiecznego, chroniącego prywatność i interoperacyjnego udostępniania sygnałów wieku.

Artykuł 31 – Obowiązki państw członkowskich

1. Państwa członkowskie ustanawiają co najmniej jeden środek elektroniczny chroniący prywatność, za pomocą którego opiekun może uzyskać i przedstawić poświadczenie odpowiedzialności rodzicielskiej w odniesieniu do małoletniego, do celów art. 26 ust. 1 lit. a), oraz zastosowania narzędzi dla opiekunów, o których mowa w art. 20. Środki te:

   a) muszą opierać się na źródłach autentycznych ustanowionych na mocy prawa krajowego;

   b) muszą być bezpłatne dla opiekuna;

   c) nie mogą wiązać się z udostępnianiem usługodawcom lub opinii publicznej jakichkolwiek informacji na temat odpowiedzialności rodzicielskiej poza potwierdzeniem, że odpowiedzialność rodzicielska istnieje.

2. Państwa członkowskie zapewniają, aby środki elektroniczne chroniące prywatność, o których mowa w ust. 1, były faktycznie dostępne dla wszystkich obywateli i opiekunów oraz małoletnich zamieszkałych na ich terytorium, w tym osób z niepełnosprawnościami, osób o ograniczonym dostępie cyfrowym lub ograniczonych umiejętnościach cyfrowych oraz osób znajdujących się w trudnej sytuacji, takich jak rodziny uchodźcze i wysiedlone.

3. Państwa członkowskie przewidują odpowiednie alternatywne procedury na potrzeby sytuacji, gdy odpowiedzialności rodzicielskiej nie można wykazać za pomocą standardowego dokumentu stanu cywilnego.

4. Państwa członkowskie wprowadzają niezbędne środki w celu zapewnienia dostępności środków umożliwiających uzyskanie poświadczenia dowodu wieku w celu weryfikacji minimalnego wieku określonego w niniejszym rozporządzeniu.

5. Państwa członkowskie wprowadzają niezbędne środki w celu zapewnienia obywatelom i rezydentom bezpłatnego dostępu do co najmniej jednego unijnego rozwiązania z zakresu weryfikacji wieku certyfikowanego zgodnie z art. 29 ust. 3 na potrzeby weryfikacji progów wieku określonych w niniejszym rozporządzeniu.

6. Państwa członkowskie zapewniają, aby organy publiczne mogły być akredytowane do celów art. 29 ust. 3, i przekazują Komisji nazwy i adresy organów publicznych wyznaczonych i akredytowanych na ich terytorium, a także informacje o wszelkich późniejszych zmianach w tym zakresie. Komisja podaje te informacje do wiadomości publicznej.

7. Państwa członkowskie bez zbędnej zwłoki powiadamiają Komisję o unijnych rozwiązaniach z zakresu weryfikacji wieku i unijnych poświadczeniach dowodu wieku certyfikowanych zgodnie z art. 29 ust. 3, wraz z odpowiednim certyfikatem zgodności, a także o każdym późniejszym zawieszeniu lub cofnięciu certyfikatu. Po umieszczeniu na listach, o których mowa w art. 29 ust. 1 lit. a) i b), unijne rozwiązanie z zakresu weryfikacji wieku i unijne poświadczenia dowodu wieku są uznawane przez wszystkie państwa członkowskie do celów niniejszego rozporządzenia.

Artykuł 32 – Istniejące konta

1. Do celów ustalenia, zgodnie z art. 6 ust. 4, czy istniejące konto należy do odbiorcy w wieku poniżej 15 lat, dostawcy, o których mowa w art. 6 ust. 1, muszą polegać na rozwiązaniu z zakresu weryfikacji wieku, o którym mowa w art. 30 ust. 2.

2. Na zasadzie odstępstwa od ust. 1 niniejszego artykułu dostawcy, o których mowa w tym ustępie, nie są zobowiązani do przeprowadzania weryfikacji wieku, jeżeli mogą wykazać z wysokim stopniem pewności, że odbiorca usługi osiągnął minimalny wiek określony w art. 6.

3. Na zasadzie odstępstwa od art. 8 ust. 1 dostawcy objęci zakresem stosowania tego artykułu oraz dostawcy sklepów z aplikacjami nie są zobowiązani do oceny wieku odbiorcy, jeżeli mogą wykazać z wysokim stopniem pewności, że odbiorca usług nie jest małoletni.

4. Dostawcy bardzo dużych platform internetowych wskazanych zgodnie z art. 33 rozporządzenia (UE) 2022/2065, którzy są objęci zakresem stosowania niniejszego artykułu, przedkładają właściwemu organowi plan, w którym określają, w jaki sposób zamierzają zapewniać zgodność z ust. 1 i art. 8 ust. 1, a w przypadku gdy zamierzają skorzystać z wyjątków określonych w ust. 2 i 3 – w jaki sposób zamierzają ustalać, że odbiorca usługi lub użytkownik systemu osiągnął minimalny wiek, zgodnie z tymi ustępami.

ROZDZIAŁ VI – ŚRODKI WSPARCIA MAŁOLETNICH

Artykuł 33 – Krajowe środki mające na celu przygotowanie i wspieranie małoletnich

1. Państwa członkowskie wspierają ochronę małoletnich poprzez ustanowienie krajowych strategii mających na celu zapewnienie małoletnim i ich opiekunom:

   a) łatwego, bezpłatnego i poufnego dostępu na szczeblu krajowym do kanałów, za pośrednictwem których małoletni mogą zwracać się o pomoc w związku ze szkodami, o których mowa w niniejszym rozporządzeniu, w tym niepożądanym kontaktem i cyberszykanowaniem;

   b) odpowiednich informacji na temat zagrożeń, których dotyczy niniejsze rozporządzenie, oraz na temat dostępnych środków ochrony, w tym poprzez odniesienie się do kwestii umiejętności cyfrowych;

   c) innych informacji istotnych dla ochrony małoletnich w internecie.

2. Działania państw członkowskich mające na celu wspieranie ochrony małoletnich muszą opierać się na doświadczeniu i wiedzy eksperckiej centrów bezpieczniejszego internetu w zakresie prowadzonych przez nie działań uświadamiających, ich telefonów zaufania wspierających dzieci, opiekunów i wychowawców oraz ich gorących linii do zgłaszania potencjalnie nielegalnych treści.

3. Państwa członkowskie komunikują Komisji strategie, o których mowa w ust. 1, do dnia [ten sam dzień co data wejścia w życie plus 12 miesięcy] r.

4. Działania, o których mowa w ust. 1, mogą być wspierane ze środków unijnych udostępnianych w ramach odpowiednich programów i instrumentów unijnych ustanowionych na podstawie wieloletnich ram finansowych.

5. Komisja ułatwia wymianę najlepszych praktyk między państwami członkowskimi, w tym w zakresie rozwoju umiejętności cyfrowych oraz tworzenia i funkcjonowania krajowych kanałów i aplikacji wsparcia.

ROZDZIAŁ VII – KOMPETENCJE, NADZÓR I EGZEKWOWANIE

Artykuł 34 – Kompetencje, nadzór i egzekwowanie

1. Do celów nadzoru i egzekwowania obowiązków nałożonych niniejszym rozporządzeniem na dostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo, gier internetowych będących platformami gier wideo oraz sklepów z aplikacjami zastosowanie ma rozdział IV rozporządzenia (UE) 2022/2065, a wszelkie zawarte w nim odniesienia do dostawcy usług pośrednich interpretuje się jako obejmujące dostawcę usług objętych niniejszym rozporządzeniem. Wszelkie zawarte w nim odniesienia do przestrzegania lub nieprzestrzegania odpowiednich przepisów rozporządzenia (UE) 2022/2065 uznaje się za obejmujące niniejsze rozporządzenie.

2. Do celów nadzoru i egzekwowania obowiązków nałożonych niniejszym rozporządzeniem na dostawców towarzyszy AI i ogólnych chatbotów konwersacyjnych zastosowanie ma rozdział IX rozporządzenia (UE) 2024/1689, a wszelkie zawarte w nim odniesienia do zgodności lub niezgodności z odpowiednimi przepisami rozporządzenia (UE) 2024/1689 interpretuje się jako obejmujące rozdziały II, III i IV niniejszego rozporządzenia. Niewypełnienie tych obowiązków podlega administracyjnym karom pieniężnym na podstawie art. 99 rozporządzenia (UE) 2024/1689, których wysokość nie przekracza 6 % całkowitego rocznego światowego obrotu przedsiębiorstwa dostarczającego towarzysza AI lub ogólnego chatbota konwersacyjnego w poprzedzającym roku obrachunkowym, jeżeli zostanie stwierdzone, że dostawca ten działał umyślnie lub w wyniku zaniedbania.

3. Państwa członkowskie zapewniają, aby organy wyznaczone przez nie zgodnie z art. 49 rozporządzenia (UE) 2022/2065 oraz art. 70 i 74 rozporządzenia (UE) 2024/1689 były właściwe do nadzoru wykonywania i egzekwowania niniejszego rozporządzenia w odniesieniu do dostawców usług lub systemów objętych niniejszym rozporządzeniem.

4. W zakresie, w jakim na podstawie rozdziału IV sekcja 4 rozporządzenia (UE) 2022/2065 oraz na podstawie art. 75a–75d i art. 99 rozporządzenia (UE) 2024/1689 powierza się Komisji uprawnienia, uprawnienia te obejmują również nadzór, czynności sprawdzające, egzekwowanie i monitorowanie przestrzegania niniejszego rozporządzenia.

5. Państwa członkowskie zapewniają, aby właściwy organ był odpowiedzialny za nadzór nad dostawcami gier internetowych będących grami wideo oraz za egzekwowanie art. 15 i mających zastosowanie przepisów art. 8 i 18–22. Taki właściwy organ posiada uprawnienia określone w art. 51 rozporządzenia (UE) 2022/2065. Do celów niniejszego ustępu państwa członkowskie ustanawiają przepisy dotyczące kar nakładanych w przypadku naruszeń art. 15 i mających zastosowanie przepisów art. 8 i 18–22, jak określono w art. 52 rozporządzenia (UE) 2022/2065. Właściwy organ państwa członkowskiego, w którym znajduje się główne miejsce prowadzenia działalności dostawcy gier internetowych będących grami wideo, ma wyłączne uprawnienia do nadzoru wykonywania i egzekwowania niniejszego rozporządzenia.

6. Organy nadzorcze, o których mowa w art. 51 rozporządzenia (UE) 2016/679, są właściwe do monitorowania przetwarzania danych osobowych niezbędnych do zapewnienia zgodności z niniejszym rozporządzeniem, w szczególności z art. 27, 28 i 29 niniejszego rozporządzenia. Za naruszenia obowiązków ochrony danych określonych w tych artykułach organy nadzorcze ds. ochrony danych mogą w ramach swoich kompetencji nakładać grzywny zgodnie z art. 83 rozporządzenia (UE) 2016/679 i do wysokości, o której mowa w art. 83 ust. 5 tego rozporządzenia.

7. Organy państw członkowskich nie mogą podejmować decyzji sprzecznych z decyzją przyjętą przez Komisję na podstawie niniejszego rozporządzenia. Komisja i państwa członkowskie, w tym koordynatorzy ds. usług cyfrowych, organy nadzoru rynku i organy krajowe odpowiedzialne za egzekwowanie przepisów prawa ochrony konsumentów, ściśle ze sobą współpracują i koordynują swoje działania.

Artykuł 35 – Tryb przyspieszony

1. Do celów rozdziału IV sekcja 4 rozporządzenia (UE) 2022/2065 i rozdziału IX rozporządzenia (UE) 2024/1689, w przypadku gdy obowiązki określone w niniejszym rozporządzeniu mają zastosowanie do dostawców bardzo dużych platform internetowych wskazanych zgodnie z art. 33 rozporządzenia (UE) 2022/2065 lub do dostawców systemów AI pod wyłącznym nadzorem Komisji zgodnie z rozporządzeniem (UE) 2024/1689, uprawnienia powierzone Komisji na podstawie rozdziału IV rozporządzenia (UE) 2022/2065 i rozdziału IX rozporządzenia (UE) 2024/1689 wykonuje się zgodnie z niniejszym artykułem.

2. W przypadku gdy Komisja wszczyna postępowanie w sprawie naruszenia niniejszego rozporządzenia zgodnie z art. 66 rozporządzenia (UE) 2022/2065 lub art. 75a rozporządzenia (UE) 2024/1689 w celu ewentualnego przyjęcia decyzji na podstawie art. 73 i 74 rozporządzenia (UE) 2022/2065 lub art. 75c rozporządzenia (UE) 2024/1689, Komisja dokłada starań, aby:

   a) zakomunikować swoje wstępne ustalenia odpowiedniemu dostawcy w terminie [30] dni roboczych od wszczęcia postępowania na podstawie art. 66 rozporządzenia (UE) 2022/2065 lub art. 75a rozporządzenia (UE) 2024/1689;

   b) wydać ostateczną decyzję w terminie 90 dni roboczych od dnia wszczęcia postępowania.

Artykuł 36 – Opłata nadzorcza

1. Komisja pobiera roczną opłatę nadzorczą od dostawców bardzo dużych platform internetowych wskazanych zgodnie z art. 33 rozporządzenia (UE) 2022/2065, które stanowią, są wbudowane w lub mają wbudowane internetowe serwisy społecznościowe, usługi platformy udostępniania wideo lub sklepy z aplikacjami, oraz od dostawców towarzyszy AI, ogólnych chatbotów konwersacyjnych i platform gier wideo, w odniesieniu do których posiada kompetencje do nadzorowania ich zgodności z rozdziałami II–V niniejszego rozporządzenia zgodnie z art. 33 niniejszego rozporządzenia.

2. Od każdego dostawcy, o którym mowa w ust. 1, pobiera się roczną opłatę nadzorczą za każdą usługę lub każdy system objęte zakresem stosowania niniejszego rozporządzenia.

3. Całkowita kwota rocznych opłat nadzorczych na podstawie ust. 1 musi pokrywać koszty poniesione przez Komisję w poprzedzającym roku kalendarzowym w związku z jej zadaniami nadzorczymi na mocy niniejszego rozporządzenia wobec dostawców usług, o których mowa w ust. 1, w szczególności koszty związane z zasobami ludzkimi, w tym z urzędnikami, ustanowieniem, utrzymaniem i funkcjonowaniem unijnego systemu weryfikacji wieku na podstawie art. 29, wykonywaniem zadań w zakresie nadzoru i egzekwowania na podstawie art. 34 oraz rozwojem wiedzy eksperckiej i zdolności na podstawie art. 37.

4. Do celów ustalenia rocznej opłaty nadzorczej za zadania wykonywane na podstawie ust. 3 roczna opłata nadzorcza pobierana od każdego z dostawców, o których mowa w ust. 1, nie przekracza 0,03 % jego światowego rocznego dochodu netto w poprzedzającym roku obrachunkowym.

5. Do celów stosowania niniejszego artykułu Komisja stosuje przepisy i zasady określone w art. 43 rozporządzenia (UE) 2022/2065.

6. Komisja przyjmuje akty delegowane, zgodnie z art. X, ustanawiające szczegółową metodykę i procedury dotyczące:

   a) określenia szacunkowych kosztów, o których mowa w ust. 3;

   b) określenia indywidualnych rocznych opłat nadzorczych, o których mowa w ust. 1;

   c) określenia maksymalnego ogólnego limitu, o którym mowa w ust. 4; oraz

   d) szczegółowych ustaleń niezbędnych do dokonywania płatności.

   Przyjmując te akty delegowane, Komisja przestrzega zasad ustanowionych w ust. 5 niniejszego artykułu.

Artykuł 37 – Rozwój wiedzy eksperckiej i zdolności

Komisja, we współpracy z właściwymi organami zgodnie z art. 34, rozwija unijną wiedzę ekspercką i zdolności w sferze ochrony małoletnich, w tym w stosownych przypadkach poprzez oddelegowanie personelu państw członkowskich. Taki rozwój wiedzy eksperckiej i zdolności następuje w szczególności w obszarze incydentów mających wpływ na ochronę małoletnich.

Artykuł 38 – Mechanizmy reagowania na incydenty

1. Komisja, we współpracy z właściwymi organami zgodnie z art. 33, koordynuje ocenę incydentów mających wpływ na ochronę małoletnich w całej Unii w odniesieniu do usług i systemów objętych zakresem stosowania niniejszego rozporządzenia oraz może polegać na wiedzy eksperckiej i zasobach takich organów. Państwa członkowskie współpracują z Komisją przy tworzeniu skutecznych sieci wymiany wiedzy z innymi organami i odpowiednimi stronami trzecimi.

2. Komisja zawiera dobrowolne porozumienie administracyjne z właściwymi organami określające procedury ułatwiające szybkie reagowanie w przypadku incydentu mającego wpływ na ochronę małoletnich w Unii lub w znacznych częściach Unii. Państwa członkowskie ustanawiają minimalne poziomy gotowości organów krajowych w celu zapewnienia kanałów regularnej komunikacji między odpowiednimi organami krajowymi a stronami trzecimi oraz mapują istniejące protokoły reagowania na incydenty na szczeblu krajowym, a w stosownych

przypadkach ustanawiają nowe protokoły. Mechanizm reagowania na incydenty musi uzupełniać istniejące narzędzia kryzysowe na podstawie rozporządzenia (UE) 2022/2065 i stanowić źródło informacji na potrzeby ich ewentualnego uruchamiania.

ROZDZIAŁ VIII – AKTY WYKONAWCZE I DELEGOWANE

Art. 39 – Wykonywanie przekazanych uprawnień

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

2. Uprawnienia, o których mowa w art. 2 ust. 5, art. 6 ust. 6, art. 7 ust. 6, art. 20 ust. 7, art. 25 ust. 1, art. 26 ust. 3, art. 30 ust. 3 i art. 36 ust. 6, powierza się Komisji na okres pięciu lat od dnia [ten sam dzień co data wejścia w życie] 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. 2 ust. 5, art. 6 ust. 6, art. 7 ust. 6, art. 20 ust. 7, art. 25 ust. 1, art. 26 ust. 3, art. 30 ust. 3 i art. 36 ust. 6, 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. 2 ust. 5, art. 6 ust. 6, art. 7 ust. 6, art. 20 ust. 7, art. 25 ust. 1, art. 26 ust. 3, art. 30 ust. 3 i art. 36 ust. 6 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 trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Art. 40 – Procedura komitetowa

1. Komisję wspomaga komitet („Komitet ds. Bezpieczeństwa Dzieci”). Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

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

3. 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.

ROZDZIAŁ IX − PRZEPISY KOŃCOWE

Artykuł 41 – Zmiana w dyrektywie (UE) 2020/1828

W załączniku I do dyrektywy (UE) 2020/1828 dodaje się punkt w brzmieniu: [ostateczna nazwa aktu].

Artykuł 42 – Przegląd

1. Komisja dokonuje przeglądu stosowania niniejszego rozporządzenia i przedkłada sprawozdanie Parlamentowi Europejskiemu i Radzie nie później niż dnia [31 sierpnia 2030] r. Biorąc pod uwagę doświadczenia zdobyte podczas stosowania niniejszego rozporządzenia, a także rozwój technologiczny, rynkowy i prawny, Komisja ocenia w szczególności:

   a) wkład niniejszego rozporządzenia w pogłębianie i skuteczne funkcjonowanie rynku wewnętrznego oraz w zapewnianie wysokiego poziomu ochrony małoletnich w internecie w Unii Europejskiej;

   b) efektywność stosowania art. 6 i 7;

   c) zakres podmiotowy przepisów rozdziałów II i III;

   d) wpływ niniejszego rozporządzenia na poszanowanie prawa do wolności wypowiedzi i informacji.

2. Do sprawozdania, o którym mowa w ust. 1, dołącza się w stosownych przypadkach wniosek dotyczący zmiany niniejszego rozporządzenia.

3. Ponadto, co cztery lata po sporządzeniu sprawozdania, o którym mowa w ust. 1, Komisja przekazuje Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące postępów w osiąganiu celów niniejszego rozporządzenia.

Artykuł 43 – Wejście w życie i rozpoczęcie stosowania

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

Niniejsze rozporządzenie stosuje się od dnia [ten sam dzień co data wejścia w życie plus 6 miesięcy] r.

Art. 5 stosuje się jednak od dnia [ten sam dzień co data wejścia w życie] r., a art. 33 i 35 stosuje się od dnia [ten sam dzień co data wejścia w życie plus 12 miesięcy] r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia r.

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

OCENA SKUTKÓW FINANSOWYCH I CYFROWYCH REGULACJI

1. KONTEKST WNIOSKU 1
- Przyczyny i cele wniosku 1
- Spójność z przepisami obowiązującymi w tej dziedzinie polityki 3
- Spójność z innymi politykami Unii 3

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ 5
- Podstawa prawna 5
- Pomocniczość (w przypadku kompetencji niewyłącznych) 5
- Proporcjonalność 6
- Wybór instrumentu 7

3. WYNIKI OCEN EX POST, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW 7
- Konsultacje z zainteresowanymi stronami 7
- Ocena skutków 9
- Prawa podstawowe 10

4. WPŁYW NA BUDŻET 12

5. ELEMENTY FAKULTATYWNE 12
- Plany wdrożenia i monitorowanie, ocena i sprawozdania 12
- Szczegółowe objaśnienia poszczególnych przepisów wniosku 12

ROZDZIAŁ I – PRZEPISY OGÓLNE 45

ROZDZIAŁ II – ODROCZENIE ZAKŁADANIA I KORZYSTANIA Z KONT PRZEZ MAŁOLETNICH W INTERNETOWYCH SERWISACH SPOŁECZNOŚCIOWYCH I USŁUGACH PLATFORMY UDOSTĘPNIANIA WIDEO 51

SEKCJA I – Odroczenie dostępu małoletnich 51

Sekcja II – Kontrolowany przez opiekuna dostęp małoletnich poniżej 13. roku życia 53

ROZDZIAŁ III – UWZGLĘDNIANIE BEZPIECZEŃSTWA NA ETAPIE PROJEKTOWANIA 55

Sekcja I – Ogólny obowiązek uwzględniania bezpieczeństwa na etapie projektowania 55

Sekcja II – Obowiązki dotyczące internetowych serwisów społecznościowych i usług platformy udostępniania wideo 55

Sekcja III – Obowiązki dotyczące towarzyszy AI i ogólnych chatbotów konwersacyjnych 59

Sekcja IV – Obowiązki dostawców gier internetowych 60

SEKCJA V – Obowiązki w zakresie dostępu dostosowanego do wieku 61

SEKCJA VI – Ogólne obowiązki dotyczące sprawczości małoletnich i narzędzia zwiększające podmiotowość małoletnich i opiekunów 63

SEKCJA VII – Inne obowiązki w zakresie należytej staranności na rzecz bezpiecznego środowiska internetowego ... 66
ROZDZIAŁ IV – WERYFIKACJA ODPOWIEDZIALNOŚCI RODZICIELSKIEJ ... 68
ROZDZIAŁ V – POTWIERDZANIE WIEKU ... 69
Sekcja I – Ogólne zasady potwierdzania wieku ... 69
Sekcja II – Szczegółowe obowiązki w zakresie potwierdzania wieku ... 70
ROZDZIAŁ VI – ŚRODKI WSPARCIA MAŁOLETNICH ... 73
ROZDZIAŁ VII – KOMPETENCJE, NADZÓR I EGZEKWOWANIE ... 74
ROZDZIAŁ VIII – AKTY WYKONAWCZE I DELEGOWANE ... 77
ROZDZIAŁ IX − PRZEPISY KOŃCOWE ... 78
1. STRUKTURA WNIOSKU/INICJATYWY ... 4
1.1. Tytuł wniosku/inicjatywy ... 4
1.2. Obszary polityki, których dotyczy wniosek/inicjatywa ... 4
1.3. Cel(e) ... 4
1.3.1. Cel(e) ogólny(-e) ... 4
1.3.2. Cel(e) szczegółowy(-e) ... 5
1.3.3. Oczekiwane wyniki i wpływ ... 5
1.3.4. Wskaźniki dotyczące realizacji celów ... 6
1.4. Wniosek/inicjatywa dotyczy: ... 7
1.5. Uzasadnienie wniosku/inicjatywy ... 7
1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy ... 7
1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tej sekcji „wartość dodaną z tytułu zaangażowania Unii Europejskiej” należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie. ... 8
1.5.3. Główne wnioski wyciągnięte z podobnych działań ... 8
1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami ... 9
1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym możliwości przegrupowania środków ... 9
1.6. Czas trwania wniosku/inicjatywy i jego/jej wpływu finansowego ... 11
1.7. Planowane metody wykonania budżetu ... 11
2. ŚRODKI ZARZĄDZANIA ... 13
2.1. Zasady nadzoru i sprawozdawczości ... 13
2.2. System zarządzania i kontroli ... 13

2.2.1. Uzasadnienie dla proponowanych metod wykonania budżetu, mechanizmów finansowania wykonania, sposobów dokonywania płatności i strategii kontroli 13
2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia 15
2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu) 16
2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom 16
3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY 17
3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ 17
3.2. Szacunkowy wpływ finansowy wniosku na środki 18
3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne 18
3.2.1.1. Środki z uchwalonego budżetu 18
3.2.1.2. Środki z zewnętrznych dochodów przeznaczonych na określony cel 18
3.2.2. Szacowany produkt finansowany ze środków operacyjnych (nie wypełniać w przypadku agencji zdecentralizowanych) 20
3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne 22
3.2.3.1. Środki z uchwalonego budżetu 22
3.2.3.2. Środki z zewnętrznych dochodów przeznaczonych na określony cel 22
3.2.3.3. Ogółem środki 22
3.2.4. Szacowane zapotrzebowanie na zasoby ludzkie 23
3.2.4.1. Finansowane z uchwalonego budżetu 23
3.2.4.2. Finansowane z zewnętrznych dochodów przeznaczonych na określony cel 24
3.2.4.3. Zapotrzebowanie na zasoby ludzkie ogółem 25
3.2.5. Przegląd szacowanego wpływu na inwestycje związane z technologiami cyfrowymi28
3.2.6. Zgodność z obowiązującymi wieloletnimi ramami finansowymi 29
3.2.7. Udział osób trzecich w finansowaniu 29
3.3. Szacunkowy wpływ na dochody 29
4. WYMIAR CYFROWY 30
4.1. Wymogi cyfrowe 31
4.2. Dane 32
4.3. Rozwiązania cyfrowe 32
4.4. Ocena interoperacyjności 32
4.5. Środki wspierające cyfrowe wdrażanie 32

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Ustawa o bezpieczeństwie i prawach dzieci w internecie (CARE)

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

Obszar polityki: ochrona małoletnich w internecie w obszarach polityki dotyczących sieci komunikacyjnych, treści i technologii; zdrowie publiczne; rynek wewnętrzny, przemysł, przedsiębiorczość i MŚP.

Wpływ na budżet dotyczy nowych zadań nadzorczych powierzonych Komisji w odniesieniu do internetowych serwisów społecznościowych, usług platformy udostępniania wideo, sklepów z aplikacjami, a także towarzyszy AI i ogólnych chatbotów konwersacyjnych wchodzących w zakres kompetencji Komisji. Pewne ograniczone skutki wynikają również z nowych obowiązków dotyczących gier wideo, chociaż bezpośredni nadzór leży w gestii organów państw członkowskich.

1.3. Cel(e)

1.3.1. Cel(e) ogólny(-e)

Proponowane rozporządzenie stanowi kontynuację wniosków ze sprawozdania współprzewodniczących specjalnego panelu ds. bezpieczeństwa dzieci w internecie, w którym określono jasną ścieżkę skuteczniejszej ochrony dzieci w Europie w środowisku internetowym.

Jak wskazano w sprawozdaniu, dzieci spędzają coraz więcej czasu w internecie i w związku z tym są podatne na wiele różnych zagrożeń, takich jak ekspozycja na treści nieodpowiednie do wieku, cyberszykanowanie, nadmierny czas spędzany w internecie oraz niepożądane kontakty ze strony nieznajomych. Zagrożenia te mają poważne konsekwencje dla zdrowia psychicznego i dobrostanu małoletnich, przy czym szczególnie wrażliwą grupą są nastolatki i dzieci.

Istnieje ryzyko, że rynek UE stanie się coraz bardziej rozdrobniony, ponieważ państwa członkowskie planują lub przyjmują nowe środki mające na celu ograniczenie dostępu do niektórych platform internetowych uznawanych za ryzykowne dla dzieci poniżej określonego wieku – z różnymi zakresami, limitami wiekowymi i proponowanymi ograniczeniami – co spowoduje niepewność prawa, wysokie koszty przestrzegania przepisów dla przedsiębiorstw i nierówny poziom ochrony małoletnich w środowisku cyfrowym, które nie zna granic.

Aby zapewnić małoletnim bezpieczne i dostosowane do wieku środowisko cyfrowe, co podkreślono również w sprawozdaniu współprzewodniczących specjalnego panelu, potwierdzanie wieku ma kluczowe znaczenie dla skutecznej ochrony małoletnich w internecie. Potwierdzanie wieku leży u podstaw zarówno limitów wiekowych, jak i środków bezpieczeństwa dla dzieci. Obecne ramy prawne dotyczące potwierdzania wieku nie są jednak przejrzyste, a ich wdrażanie jest niejednolite.

W tym kontekście proponowane rozporządzenie ma na celu zapewnienie **silnych i spójnych ram ochrony małoletnich w internecie**, przyjmując za punkt wyjścia dziecko i wzmocnienie jego pozycji oraz prawa podstawowe.

1.3.2. Cel(e) szczegółowy(-e)

Biorąc pod uwagę ogólny cel, jakim jest ochrona małoletnich w internecie, wniosek służy realizacji następujących celów szczegółowych:

Opóźnienie dostępu małoletnich do usług o szczególnych cechach, które stanowią usługi sieci społecznościowych lub platformy udostępniania wideo. W przypadku tych usług nie zezwala się małoletnim poniżej 15. roku życia na założenie konta. Dostawcy tych usług mogą zezwolić opiekunom na zakładanie kont dla małoletnich w wieku powyżej 13 lat z ograniczonymi funkcjami w celu uzyskania dostępu do usługi. W przypadku gdy tacy dostawcy mogą wykazać, że są usługą przyjazną dziecku, mogą oni udzielić dostępu również małoletnim poniżej 13. roku życia za pośrednictwem kont utworzonych i nadzorowanych przez ich opiekuna.

Wzmocnienie ochrony małoletnich poprzez wymogi uwzględniania bezpieczeństwa na etapie projektowania poprzez doprecyzowanie obowiązków w zakresie usług cyfrowych i niektórych systemów, tak aby przy projektowaniu i funkcjonowaniu tych usług i systemów uwzględniano zagrożenia dla dzieci.

Zapewnienie wiarygodnych i zgodnych z prawami podstawowymi mechanizmów potwierdzania wieku poprzez ustanowienie jasnych wymogów i kryteriów stosowania systemów potwierdzania wieku w celu wsparcia zarówno odroczenia dostępu, jak i wdrażania środków uwzględniania bezpieczeństwa na etapie projektowania.

Zapewnienie skutecznego egzekwowania przepisów w całej UE poprzez ustanowienie solidnych i spójnych ram regulacyjnych i ram egzekwowania przepisów, które umożliwią ich terminowe i skuteczne wdrażanie, zapewniając szybką i skuteczną ochronę małoletnich w praktyce.

1.3.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Oczekuje się, że wniosek przyczyni się do stworzenia bezpieczniejszego środowiska internetowego dla dzieci, a jednocześnie poprawi funkcjonowanie rynku wewnętrznego. Dzięki doprecyzowaniu i dalszej harmonizacji obowiązków w zakresie ochrony dzieci w całej Unii wniosek powinien zmniejszyć fragmentację regulacyjną i zapewnić bardziej przewidywalne ramy transgranicznego świadczenia usług i zapewniania systemów, w szczególności biorąc pod uwagę transgraniczny charakter dostawców objętych zakresem niniejszego rozporządzenia.

W perspektywie krótkoterminowej w przypadku dostawców usług i systemów, których to dotyczy, wniosek może zwiększyć wewnętrzne koszty przestrzegania przepisów, wymagać przeprojektowania produktów i wdrożenia dodatkowych środków bezpieczeństwa – takich jak potwierdzanie wieku lub narzędzia kontroli dla opiekunów – oraz może stworzyć pewne bariery wejścia dla niektórych dostawców. Oczekuje się jednak, że z czasem jaśniejsze zobowiązania prawne spowodują obniżenie kosztów, zapewnią bardziej wyrównane warunki konkurencji oraz ułatwią nadzór i egzekwowanie przepisów przez organy publiczne, przy czym przewiduje się, że ogólne skutki dla organów publicznych będą neutralne lub umiarkowanie pozytywne.

Wniosek ma również zachęcać do innowacji w zakresie projektowania bezpiecznego dla dzieci oraz dostosowanych do wieku usług i systemów cyfrowych, w tym rozwiązań w zakresie potwierdzania wieku chroniących prywatność. Chociaż koszty weryfikacji wieku lub alternatywnego potwierdzania wieku wzrosną, synergie z szerszą unijną infrastrukturą cyfrową, w szczególności z unijnym portfelem tożsamości cyfrowej i unijnym planem weryfikacji wieku, mogą z czasem zmniejszyć koszty wdrażania.

1.3.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

Określono następujące główne wskaźniki:

Ograniczenie dostępu do usług i systemów cyfrowych wysokiego ryzyka: Szereg badań wskazuje, że w UE miliony małoletnich poniżej 13. roku życia korzystają z mediów społecznościowych i mają własne konta (1). Na przykład w sześciu krajach 34 % osób w wieku 9–11 lat zgłasza posiadanie profilu w mediach społecznościowych (2). W tym kontekście celem byłoby zapewnienie, aby znaczna część usług stosowała skuteczne ograniczenia dostępu zgodnie z nowymi wymogami. Niedawne doświadczenia w Australii pokazują, że taka zmiana społeczna wymaga czasu i nie tylko skutecznego przestrzegania przepisów przez dostawców, ale także transformacji z udziałem małoletnich, rodziców i całego społeczeństwa. W związku z tym powodzenie będzie wymagało skutecznego egzekwowania przepisów, podnoszenia świadomości w społeczeństwie, szerokiego zaangażowania społecznego, stałego monitorowania i uznania, że zmiana zachowań wymaga czasu.

Wdrożenie wymogów uwzględniania bezpieczeństwa na etapie projektowania: Obecnie środowisko internetowe nie jest projektowane z myślą o dzieciach i nie uwzględnia ich zmieniających się zdolności. W internecie dzieci są podatne na wiele zagrożeń, które mogą mieć poważny wpływ na ich dobrostan, rozwój oraz zdrowie fizyczne i psychiczne. Zagrożenia te stale się zmieniają, a ponieważ dzieci jako pierwsze zaczynają korzystać z nowych technologii, pozostają one również najbardziej podatne na związane z nimi zagrożenia. W tym kontekście celem byłoby zapewnienie, aby środowisko internetowe stało się bezpieczniejsze dla małoletnich dzięki wdrożeniu środków uwzględniania bezpieczeństwa na etapie projektowania. Powodzenie będzie wymagało, aby bezpieczeństwo małoletnich było uwzględniane w produktach i usługach od samego początku i przez cały cykl życia produktu lub usługi, co doprowadzi do ogólnej transformacji regulowanych usług i systemów, w których ochronę małoletnich należy traktować priorytetowo. Powinno to być połączone ze skutecznym egzekwowaniem i nadzorem.

Wprowadzenie zgodnych z prawami podstawowymi systemów potwierdzania wieku. Istniejące wymogi wiekowe na platformach internetowych zazwyczaj nie są opracowywane w oparciu o potrzeby dzieci i praktycznie nie są egzekwowane. Większość dostawców usług cyfrowych określa w swoich warunkach korzystania z usług minimalny wiek dostępu do swoich usług lub ich użytkowania (3). Jak zauważyła OECD, wybór wieku przez platformę wynika z przyczyn związanych z prywatnością i prawem umów, a nie z oceny bezpieczeństwa lub adekwatności pod względem rozwoju (4). OECD podkreśla ponadto, że „bardzo niewiele [usług, które określają minimalny wiek w warunkach korzystania z usług] wdraża systemowe potwierdzanie wieku" oraz że tylko 2 z 50 analizowanych usług online systematycznie wymagają potwierdzenia wieku do założenia konta (5). Jedyną formą

kontroli wieku przed założeniem konta jest zazwyczaj oświadczenie własne. Powszechnie uznaje się, że samo oświadczenie własne nie jest skutecznym środkiem potwierdzania wieku, ponieważ wielu użytkowników nie ujawnia swojego rzeczywistego wieku (6, 7, 8). Szereg badań pokazuje, że małoletni rutynowo podają nieprawdziwy wiek w internecie (9). W praktyce niepełnoletni użytkownicy mogą zatem z łatwością uzyskać dostęp do wielu usług online ograniczonych wiekiem. W tym kontekście celem jest szerokie wykorzystanie praw podstawowych przy zachowaniu wymogu potwierdzania wieku. Można to osiągnąć poprzez działania i faktyczną zgodność ze strony usług objętych zakresem rozporządzenia, w połączeniu ze skutecznym nadzorem i egzekwowaniem, a także stałym monitorowaniem i oceną, zwłaszcza w odniesieniu do wpływu na prawa podstawowe.

Wzmocnienie skutecznego egzekwowania przepisów. Egzekwowanie rozporządzenia (UE) 2022/2065 przebiega w odpowiednim tempie, w tym w obszarze ochrony małoletnich. Przyjęcie ostatecznej decyzji stwierdzającej niewypełnianie obowiązków nadal jednak wymaga czasu. W tym kontekście, w przypadku podejrzenia niezgodności, celem jest jej pilne rozwiązanie, aby zapewnić małoletnim szybkie podjęcie skutecznych działań w celu ich ochrony w środowisku internetowym.

1.4. Wniosek/inicjatywa dotyczy:

X nowego działania

☐ nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego [10]

X przedłużenia bieżącego działania

☐ połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Ochrona małoletnich w internecie wymaga zarówno natychmiastowych działań w celu przeciwdziałania nagłym zagrożeniom, jak i środków strukturalnych, aby z czasem stworzyć bezpieczniejsze środowisko cyfrowe.

W perspektywie krótkoterminowej należy nadać priorytet skutecznemu wdrażaniu i egzekwowaniu przepisów, tak aby małoletni byli skutecznie chronieni w internecie – aby tak się stało, trzeba będzie zaangażować znaczne zasoby. Działania te należy połączyć z ukierunkowanymi środkami wsparcia i kampaniami informacyjnymi prowadzonymi przez państwa członkowskie na rzecz małoletnich, opiekunów i wychowawców.

W perspektywie długoterminowej celem jest nie tylko reagowanie na zagrożenia, ale również przekształcenie środowiska internetowego, tak aby ochrona małoletnich była zapewniona jako jego nieodłączna cecha, a nie jako środek naprawczy. Wymaga to

[10] O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

stałych inwestycji w rozwiązania w zakresie potwierdzania wieku chroniące prywatność, wysokich umiejętności cyfrowych w państwach członkowskich oraz ogólnego rozwoju usług przyjaznych dzieciom.

Sześć miesięcy po rozpoczęciu stosowania rozporządzenia dostawcy będą musieli dotrzymać terminu rozpoczęcia korzystania z mediów społecznościowych, ustalając, czy konta należą do odbiorców poniżej minimalnego wieku, i podjąć działania w celu ich dezaktywacji. W celu zapewnienia zgodności istniejących kont z wymogami dotyczącymi dolnej granicy wieku dostawcy bardzo dużych platform internetowych przed upływem sześciomiesięcznego okresu przedłożą właściwemu organowi szczegółowy plan wdrażania, który potwierdzi wymagany wysoki stopień zaufania.

Od tego dnia platformy muszą również spełniać obowiązki w zakresie uwzględniania bezpieczeństwa na etapie projektowania oraz, w razie potrzeby, stosować weryfikację wieku. Jednocześnie sześć miesięcy po rozpoczęciu stosowania Komisja musi być gotowa do egzekwowania nowych przepisów dotyczących bardzo dużych platform internetowych (VLOP) i wyszukiwarek (VLOSE) oraz krajowych koordynatorów ds. usług cyfrowych w odniesieniu do mniejszych platform i gier wideo. Egzekwowanie nowych wymogów dotyczących towarzyszy AI i chatbotów będzie odbywać się na podstawie istniejących ram nadzoru i egzekwowania przepisów aktu w sprawie AI, w których Komisja jest odpowiedzialna za wirtualnych asystentów AI i chatboty oparte na modelach AI ogólnego przeznaczenia lub zintegrowane z bardzo dużymi platformami internetowymi lub bardzo dużymi wyszukiwarkami internetowymi.

Dwanaście miesięcy po rozpoczęciu stosowania dostawcy usług i systemów objętych zakresem będą musieli umożliwić prowadzenie kont rodzicielskich, przestrzegać przepisów dotyczących towarzyszy AI i ogólnych chatbotów konwersacyjnych, wdrożyć różne środki wspierające, a także przestrzegać kodeksu postępowania w zakresie klasyfikacji wiekowej, jeżeli ma on do nich zastosowanie. Począwszy od tej daty, tj. 12 miesięcy po rozpoczęciu stosowania rozporządzenia, Komisja musi być gotowa do stosowania nowego przyspieszonego systemu egzekwowania przepisów (30 dni na dokonanie wstępnych ustaleń, 90 dni na podjęcie ostatecznej decyzji).

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tej sekcji „wartość dodaną z tytułu zaangażowania Unii Europejskiej" należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Działanie UE jest uzasadnione transgranicznym charakterem usług cyfrowych i systemów AI, fragmentarycznymi podejściami krajowymi dotyczącymi ograniczania dostępu małoletnich oraz potrzebą zapewnienia spójnego poziomu ochrony małoletnich w całej Unii. Wysiłki na szczeblu UE mogą zmniejszyć rozbieżności regulacyjne, zwiększyć pewność prawa i zmniejszyć koszty przestrzegania przepisów ponoszone przez dostawców i użytkowników, poprawić egzekwowanie przepisów oraz zapewnić skuteczną ochronę małoletnich w całej UE.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Na podstawie rozporządzenia (UE) 2022/2065 wyciągnięto następujące wnioski:

Kluczowe znaczenie mają wystarczające i stabilne zasoby. Doświadczenie zdobyte na podstawie rozporządzenia (UE) 2022/2065 pokazuje, że skuteczne egzekwowanie przepisów wobec największych przedsiębiorstw na świecie wymaga wysoko wykwalifikowanych zasobów, zdolności technicznych i wystarczającej liczby pracowników. Jest to szczególnie ważne przy nadzorowaniu i egzekwowaniu dużych transgranicznych usług cyfrowych, a także w środowisku, w którym często dochodzi do sporów sądowych.

Zasoby powinny być stałe. Egzekwowanie przepisów w środowisku cyfrowym powinno opierać się na stabilnych zasobach, aby zapewnić długoterminową niezawodność i przewidywalność. Ryzyko związane z usługami cyfrowymi dynamicznie się zmienia, a platformy szybko modyfikują swoje systemy, podczas gdy nadzór musi być ciągły i odporny na ryzyko efektu „drzwi obrotowych". Tylko dzięki stałym zasobom nadzór może pozostawać silny i wiarygodny z upływem czasu.

Szybkie egzekwowanie przepisów ma kluczowe znaczenie w środowisku internetowym, zwłaszcza w przypadku małoletnich. W przypadku usług cyfrowych szkody mogą szybko rosnąć, a opóźnienia mogą znacznie zmniejszyć skuteczność interwencji. W związku z tym ramy egzekwowania muszą umożliwiać podejmowanie działań w odpowiednim czasie, w tym zdolność do szybkiego reagowania w przypadku pojawienia się poważnych zagrożeń.

Wiarygodne egzekwowanie przepisów wzmacnia ich przestrzeganie. W przypadku gdy organy dysponują zdolnościami i narzędziami do zdecydowanego działania, stwarza to zachęty dla dostawców do poważnego zaangażowania się i bardziej proaktywnego przestrzegania przepisów. Skuteczny nadzór polega zatem na zapewnieniu praktycznego wpływu przepisów.

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

Inicjatywa jest zgodna z obowiązującymi wieloletnimi ramami finansowymi.

W ramach inicjatywy pobierana będzie opłata nadzorcza uiszczana przez wszystkich dostawców internetowych serwisów społecznościowych, usług platformy udostępniania wideo i sklepów z aplikacjami, w odniesieniu do których Komisja ma kompetencje do nadzorowania zgodności i które wskazano jako bardzo dużą platformę internetową na podstawie art. 33 rozporządzenia (UE) 2022/2065, oraz dostawców towarzyszy AI i ogólnych chatbotów konwersacyjnych, którzy kwalifikują się jako bardzo duża platforma internetowa. Roczna opłata nadzorcza zostanie obliczona na podstawie art. 43 rozporządzenia (UE) 2022/2065 i nie zostanie jednak podwyższona w odniesieniu do danego dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki o więcej niż 0,03 % jego światowego rocznego dochodu netto w poprzednim roku obrotowym.

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym możliwości przegrupowania środków

Preferowany wariant finansowania stanowi uzupełnienie istniejącej opłaty nadzorczej przewidzianej w akcie o usługach cyfrowych. W tym celu dostawcy internetowych serwisów społecznościowych, usług platformy udostępniania wideo i sklepów z aplikacjami, którzy są objęci nadzorem Komisji Europejskiej i którzy zostali wyznaczeni jako bardzo duża platforma internetowa na podstawie rozporządzenia (UE) 2022/2065, oraz towarzysze AI i ogólne chatboty

konwersacyjne, którzy kwalifikują się jako bardzo duża platforma internetowa, będą obciążani dodatkową opłatą w stosunku do rocznej opłaty nadzorczej na podstawie art. 43 rozporządzenia (UE) 2022/2065.

Do celów egzekwowania przepisów w ramach niniejszej inicjatywy Komisja będzie częściowo polegać na przesunięciach. Wykonywanie istotnych nowych zadań nadzorczych bez narażania na szwank istniejących prac w zakresie egzekwowania prawa wyklucza jednak poleganie wyłącznie na przesunięciach. Zob. również sekcja 4.1 załącznika.

W przypadku gdy egzekwowanie opiera się na opłatach nadzorczych, należy zauważyć, że wystąpi nieunikniona luka między początkowym zapotrzebowaniem na zasoby ludzkie a wkładem finansowym pochodzącym z opłaty nadzorczej, który będzie dostępny dopiero po wejściu w życie rozporządzenia i uiszczeniu opłaty. Luka ta stanowi poważne zagrożenie dla prawidłowego wdrożenia wniosku, ponieważ niezbędne zasoby nie będą dostępne w momencie zapotrzebowania na nie, tj. od momentu wejścia w życie. Oczekiwania polityczne i społeczne dotyczące skutecznego nadzoru i egzekwowania przepisów w celu ochrony małoletnich w internecie są wysokie, a Komisja będzie musiała w przekonujący sposób wykazać, że jest w stanie ukrócić szkodliwe zachowania. W związku z tym niezwykle ważne jest zminimalizowanie ryzyka wynikającego z luki między początkowym zapotrzebowaniem na zasoby ludzkie a wkładem finansowym pochodzącym z pierwotnej opłaty oraz zapewnienie Komisji odpowiednich zasobów do egzekwowania wniosku od pierwszego dnia jego wejścia w życie.

1.6. Czas trwania wniosku/inicjatywy i jego/jej wpływu finansowego

☐ **Ograniczony czas trwania**

– ☐ Czas trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Czas trwania wpływu finansowego: od RRRR r. do RRRR r. w odniesieniu do środków na zobowiązania oraz od RRRR r. do RRRR r. w odniesieniu do środków na płatności.

X Nieograniczony czas trwania

– Wprowadzenie w życie z okresem rozruchu od 2028 r. przez czas nieokreślony,

– po którym następuje faza operacyjna.

1.7. Planowane metody wykonania budżetu[11]

X Bezpośrednie zarządzanie przez Komisję

– **X** w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii

– ☐ przez agencje wykonawcze

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie pośrednie** przez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym

– ☐ organizacjom międzynarodowym i ich agencjom (wyszczególnić)

– ☐ Europejskiemu Bankowi Inwestycyjnemu i Europejskiemu Funduszowi Inwestycyjnemu

– ☐ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego

– ☐ organom prawa publicznego

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, w zakresie, w jakim są im zapewnione odpowiednie gwarancje finansowe

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego i zapewniono odpowiednie gwarancje finansowe

– ☐ podmiotom lub osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym

– ☐ podmiotom mającym siedzibę w państwie członkowskim, podlegającym prawu prywatnemu państwa członkowskiego lub prawu Unii i kwalifikującym się, zgodnie z przepisami sektorowymi, do powierzenia im wykonywania środków finansowych Unii lub gwarancji budżetowych, w zakresie, w jakim podmioty te

[11] Szczegóły dotyczące metod wykonania budżetu oraz odniesienia do rozporządzenia finansowego znajdują się na stronie BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

są kontrolowane przez podmioty prawa publicznego lub podmioty podlegające prawu prywatnemu świadczące usługi użyteczności publicznej, a także posiadają odpowiednie gwarancje finansowe w formie odpowiedzialności solidarnej organów kontrolnych lub równoważne gwarancje finansowe, które mogą być ograniczone, w odniesieniu do każdego działania, do maksymalnej kwoty wsparcia Unii.

Uwagi

Brak

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Wniosek zostanie poddany rygorystycznej ocenie, w szczególności pod względem skuteczności odroczenia dostępu, zakresu podmiotowego odroczenia dostępu i jego proporcjonalności oraz wymogów uwzględniania bezpieczeństwa na etapie projektowania. Ocena ta będzie uwzględniać doświadczenie zdobyte podczas wdrażania wniosku, a także zmiany technologiczne, rynkowe i prawne. Komisja będzie monitorować stosowanie niniejszego rozporządzenia i przekaże sprawozdanie Parlamentowi Europejskiemu i Radzie do dnia 31 sierpnia 2030 r.

W odpowiednich przypadkach do sprawozdania dołączany będzie wniosek w sprawie zmiany rozporządzenia. Po tym wstępnym przeglądzie Komisja będzie co cztery lata przedkładać Parlamentowi Europejskiemu i Radzie kolejne sprawozdanie z postępów w osiąganiu celów rozporządzenia.

Uzupełni to bieżące monitorowanie na podstawie aktu o usługach cyfrowych.

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla proponowanych metod wykonania budżetu, mechanizmów finansowania wykonania, sposobów dokonywania płatności i strategii kontroli

Rozporządzenie ustanawia bezpieczniejsze środowisko internetowe dla dzieci, poprawiając jednocześnie funkcjonowanie rynku wewnętrznego. Określono w nim jasne przepisy mające na celu ograniczenie dostępu małoletnich do usług i systemów cyfrowych, które stwarzają dla nich największe ryzyko, wzmocnienie ochrony małoletnich poprzez wymogi uwzględniania bezpieczeństwa na etapie projektowania, ustanowienie przejrzystych wymogów i kryteriów stosowania systemów potwierdzania wieku w celu wsparcia zarówno odroczenia dostępu, jak i wdrażania środków uwzględniania bezpieczeństwa na etapie projektowania, a także wprowadzenie skutecznego egzekwowania przepisów w całej UE poprzez ustanowienie solidnych i spójnych ram regulacyjnych i wykonawczych.

Aby Komisja mogła wykonywać powierzone jej nowe obowiązki, konieczne jest zapewnienie służbom Komisji odpowiednich zasobów. Jest to szczególnie ważne, ponieważ wykonując swoje zadania, Komisja będzie musiała nadzorować niektóre z najsilniejszych finansowo i najbardziej zaawansowanych technologicznie przedsiębiorstw na świecie, w środowisku, w którym często dochodzi do sporów sądowych. Nadzór nad tymi przedsiębiorstwami będzie wymagał pracowników o wysokich kwalifikacjach i specjalistycznych profilach. Komisja jest narażona na znaczne ryzyko polityczne w przypadku niedostatecznych zasobów na egzekwowanie przepisów, zwłaszcza że instrument ten dotyczy ochrony małoletnich, będących jednymi z najsłabszych członków społeczeństwa. Coraz częściej wzywa się do podjęcia pilnych działań w celu ochrony europejskich dzieci w internecie, a zapewnienie skutecznej ochrony następnemu pokoleniu wymaga odpowiedniego personelu, zwłaszcza aby umożliwić Komisji szybkie egzekwowanie przepisów, które będzie wymagane na mocy nowego instrumentu ustawodawczego w celu odpowiedniej i pilnej ochrony dzieci.

Szacuje się, że wdrożenie i egzekwowanie rozporządzenia będzie wymagało łącznie 85 EPC. Proponowane poziomy zatrudnienia są proporcjonalne do zakresu

i złożoności nowych obowiązków i stanowią najbardziej opłacalny wariant bez powielania działań na szczeblu krajowym.

Aby zapewnić dostępność tych zasobów, Komisja przesunie 45 EPC. Ponadto, aby uzupełnić potrzeby w zakresie zasobów i realizować istotne nowe zadania nadzorcze w ramach tego instrumentu, Komisja będzie potrzebować 40 EPC nowych pracowników.

Aby sfinansować nadzór nad przepisami w ramach tego instrumentu, Komisja będzie polegać na „dopłacie” do istniejącej opłaty nadzorczej przewidzianej w akcie o usługach cyfrowych, którą będą musieli uiścić dostawcy objęci zakresem nowego instrumentu, którzy są określeni jako VLOP na mocy aktu o usługach cyfrowych.

Podobnie jak akt o usługach cyfrowych niniejszy wniosek ustawodawczy spełnia trzy łączne wymogi dotyczące polegania na opłacie:

- Usługa jest świadczona: Usługa dotyczy nadzoru nad działalnością, tj. nadzoru nad zgodnością z rozporządzeniem. Nadzór przynosi odczuwalne korzyści dotyczące przestrzegania przepisów podmiotom objętym zakresem. Na przykład w przypadku gdy dostawcy mogą wykazać, że są usługą przyjazną dziecku, mogą udzielić dostępu również małoletnim poniżej 13. roku życia za pośrednictwem kont utworzonych i nadzorowanych przez ich opiekuna. Koszty związane ze świadczeniem usługi obejmują koszty narzędzi informatycznych, koszty personelu i inne koszty administracyjne.

- Usługa jest odbierana indywidualnie przez osoby uiszczające opłatę: Usługa zapewnia bezpośrednie korzyści podmiotom, od których wymaga się uiszczenia opłaty. Poddając się nadzorowi przewidzianemu we wniosku, dostawcy mogą wiarygodnie udowodnić, że oferują usługę bezpieczną dla małoletnich. Dopłata uzupełniająca opłatę nadzorczą przewidzianą w akcie o usługach cyfrowych w ramach tego instrumentu będzie uiszczana wyłącznie przez te podmioty, które są objęte zakresem nowego instrumentu i w związku z wyznaczeniem ich jako bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych na podstawie aktu o usługach cyfrowych podlegają bezpośredniemu nadzorowi Komisji.

- Proporcjonalny poziom opłaty: Zgodnie z ustaloną praktyką na podstawie aktu o usługach cyfrowych poziom opłaty (oraz dopłaty uzupełniającej) będzie ustalany corocznie i – pod względem wielkości – dostosowywany do poszczególnych nadzorowanych podmiotów za pomocą wzoru, który uwzględnia liczbę użytkowników usługi oraz może być i jest ograniczony do poziomu światowego zysku dostawcy usług w poprzednim roku obrotowym. Maksymalna dopłata uzupełniająca do działań nadzorczych w ramach tego nowego instrumentu w odniesieniu do danego dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej jest ograniczona do 0,03 % jego światowego rocznego dochodu netto w poprzednim roku obrotowym.

Podobnie jak w przypadku aktu o usługach cyfrowych instrument ten stanowi przypadek, w którym można zapewnić stały charakter dochodów i stały charakter zadań wykonywanych w zamian za opłatę. Opłata nadzorcza przewidziana w akcie o usługach cyfrowych jest pobierana od 2024 r. Do tej pory wynosiła ona od 40 do 60 mln EUR rocznie, przy czym niewielkie różnice można wytłumaczyć zmianami przewidywanych kosztów nadzoru na kolejny rok. Pula VLOPSE (> 45

mln aktywnych użytkowników miesięcznie) nadal rosła, a nie zmniejszała się, ponieważ więcej usług przekracza próg liczby użytkowników. Podstawę przychodów, na której opiera się nowa opłata, można zatem uznać za stabilną, ponieważ jest mało prawdopodobne, aby usługi z > 45 mln aktywnych użytkowników miesięcznie szybko straciły liczbę użytkowników i zostały usunięte spod nadzoru Komisji.

Stały charakter opłaty przewidzianej w akcie o usługach cyfrowych w połączeniu ze stałym charakterem i znaczeniem zadań nadzorczych Komisji w odniesieniu do bezpieczeństwa i wiarygodności platform internetowych, w tym ochrony dzieci w internecie, sprawia, że akt o usługach cyfrowych i obecny instrument są odpowiednim przykładem obszaru, w którym opłata bazowa mogłaby finansować stanowiska w planie zatrudnienia.

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

Działania zaproponowane w rozporządzeniu obejmują prowadzenie działań nadzorczych przez Komisję i organy krajowe. Komisja będzie musiała zapewnić wystarczającą liczbę pracowników na potrzeby takich działań, a także gotowość do przygotowania aktów delegowanych i wykonawczych, wytycznych, obsługi sekretariatu procedury komitetowej, w tym monitorowania w odniesieniu do ustalonych kluczowych wskaźników efektywności i celów pośrednich. Umożliwiłoby to szybką identyfikację ewentualnych problemów i zagrożeń związanych z realizacją działań.

Ponadto w odniesieniu do dochodów pochodzących z opłaty nadzorczej w rozporządzeniu przewidziane zostaną regularne obowiązki sprawozdawcze Komisji w zakresie poniesionych kosztów i uzyskanych dochodów.

Należy jednak zauważyć, że wystąpi nieunikniona luka między początkowym zapotrzebowaniem na zasoby ludzkie a wkładem finansowym pochodzącym z opłaty nadzorczej, który stanie się dostępny dopiero po wejściu w życie rozporządzenia i uiszczeniu opłaty.

Luka ta stanowi poważne zagrożenie dla prawidłowego wdrożenia niniejszego rozporządzenia, ponieważ niezbędne zasoby nie będą dostępne w momencie zapotrzebowania na nie, tj. od momentu wejścia w życie. Oczekiwania polityczne i społeczne dotyczące skutecznego nadzoru i egzekwowania przepisów pozwalającego osiągnąć cele niniejszego rozporządzenia są wysokie, a Komisja będzie musiała w przekonujący sposób wykazać, że jest w stanie kontrolować zachowania i wprowadzać zmiany w uzasadnionych przypadkach.

W związku z tym niezwykle ważne jest zminimalizowanie ryzyka wynikającego z luki między początkowym zapotrzebowaniem na zasoby ludzkie a wkładem finansowym pochodzącym z pierwotnej opłaty oraz zapewnienie Komisji odpowiednich zasobów do egzekwowania nowej inicjatywy od pierwszego dnia jej wejścia w życie. Przesunięcie istniejącego personelu do części działań nadzorczych w ramach tej nowej inicjatywy jest w tym względzie kluczową strategią łagodzącą.

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

Koszty kontroli związanych z tą inicjatywą oszacowano na poziomie Komisji. Źródłem tych informacji jest wewnętrzny system zarządzania i kontroli Komisji. Koszty oszacowano na podstawie personelu i zasobów przeznaczonych na działania przewidziane w ramach tej inicjatywy. Oczekiwane łączne koszty takich kontroli mogą być stosunkowo wysokie ze względu na złożoność proponowanych działań oraz konieczność przeznaczenia specjalnych zasobów na ograniczenie ryzyka związanego z ich realizacją. Intensywność kontroli zostanie dostosowana do charakteru wydatków, rodzaju przewidywanych beneficjentów lub wykonawców, wysokości odnośnych środków finansowych oraz poziomu ryzyka.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Dodatkowe potrzeby w zakresie środków niezbędnych do celów niniejszego rozporządzenia zostaną zaspokojone w ramach istniejących środków zapobiegania nadużyciom finansowym mających zastosowanie do Komisji. Ponadto niniejsze rozporządzenie będzie przewidywać regularne składanie sprawozdań na temat poniesionych kosztów i dochodów uzyskanych z opłaty nadzorczej oraz mechanizmy dostosowania poziomu opłat do poniesionych kosztów.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

Szacunkowy wpływ na wydatki i personel w 2028 r. i w kolejnych latach podano w celach ilustracyjnych i nie przesądza on o kolejnych wieloletnich ramach finansowych. Źródło finansowania i zakres zaangażowania finansowego Unii po 2027 r. pozostają zależne od wyniku negocjacji międzyinstytucjonalnych w sprawie WRF na lata 2028–2034, a następnie będą określane w drodze corocznej procedury budżetowej. Wszystkie środki i przydziały kadrowe począwszy od 2028 r. są orientacyjne.

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn. / niezróżn.[12]	państw EFTA[13]	krajów kandydujących i potencjalnych kandydatów[14]	innych państw trzecich	pochodzący z pozostałych dochodów przeznaczonych na określony cel
	02 20 03 05 Akt o usługach cyfrowych – Nadzór nad bardzo dużymi platformami internetowymi	Zróżn.	NIE	NIE	NIE	TAK

- Proponowane nowe linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn. / niezróżn.	państw EFTA	krajów kandydujących i potencjalnych kandydatów	innych państw trzecich	pochodzący z pozostałych dochodów przeznaczonych na określony cel

[12] Środki zróżnicowane/środki niezróżnicowane.

[13] EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

[14] Kraje kandydujące oraz, w stosownych przypadkach, potencjalni kandydaci z Bałkanów Zachodnich.

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej

3.2.1.1. Środki z uchwalonego budżetu

3.2.1.2. Środki z zewnętrznych dochodów przeznaczonych na określony cel

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	

DG ds. Sieci Komunikacyjnych, Treści i Technologii			Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**OGÓŁEM WRF 2028–2034**
Środki operacyjne										
Opłata przewidziana w akcie o usługach cyfrowych	Środki na zobowiązania	(1a)	7,700	5,700	5,700	5,700	5,700	5,700	5,700	**41,900**
	Środki na płatności	(2a)	5,700	5,700	7,700	5,700	5,700	5,700	5,700	**41,900**
Linia budżetowa	Środki na zobowiązania	(1b)								**0**
	Środki na płatności	(2b)								**0**
Środki administracyjne finansowane ze środków przydzielonych na określone programy[15]										
Linia budżetowa		(3)								**0**

[15] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

OGÓŁEM środki	Środki na zobowiązania	=1a+1b+3	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
dla DG CONNECT	Środki na płatności	=2a+2b+3	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

			Rok	Rok	Rok	Rok	Rok	Rok	Rok	**OGÓŁEM WRF 2028–2034**
			2028	**2029**	**2030**	**2031**	**2032**	**2033**	**2034**	
OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)	7,700	5,700	5,700	5,700	5,700	5,700	5,700	**41,900**
	Środki na płatności	(5)	5,700	5,700	7,700	5,700	5,700	5,700	5,700	**41,900**
OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy		(6)	0	0	0	0	0	0	0	**0**
OGÓŁEM środki na DZIAŁ <….> wieloletnich ram finansowych	Środki na zobowiązania	=4+6	7,700	5,700	5,700	5,700	5,700	5,700	5,700	**41,900**
	Środki na płatności	=5+6	5,700	5,700	7,700	5,700	5,700	5,700	5,700	**41,900**

Dział wieloletnich ram finansowych	4	„Wydatki administracyjne”[16]

w mln EUR (do trzech miejsc po przecinku)

DG ds. Sieci Komunikacyjnych, Treści i Technologii	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**OGÓŁEM WRF 2028–2034**
• Zasoby ludzkie	2,020	2,020	2,020	2,020	2,020	2,020	2,020	**14,140**
• Pozostałe wydatki administracyjne	0	0	0	0	0	0	0	**0**

[16] Niezbędne środki należy określić na podstawie danych dotyczących średnich rocznych kosztów, dostępnych na odpowiedniej stronie internetowej BUDGpedia.

OGÓŁEM DG CONNECT	Środki	2,020	2,020	2,020	2,020	2,020	2,020	2,020	**14,140**

OGÓŁEM środki na DZIAŁ 4 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**14,140**

w mln EUR (do trzech miejsc po przecinku)

		Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**OGÓŁEM WRF 2028–2034**
OGÓŁEM środki na DZIAŁY od 1 do 4	Środki na zobowiązania	**9,720**	**7,720**	**7,720**	**7,720**	**7,720**	**7,720**	**7,720**	**56,040**
wieloletnich ram finansowych	Środki na płatności	**7,720**	**7,720**	**9,720**	**7,720**	**7,720**	**7,720**	**7,720**	**56,040**

3.2.2. Szacowany produkt finansowany ze środków operacyjnych (nie wypełniać w przypadku agencji zdecentralizowanych)

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty ⇩			Rok **2028**		Rok **2029**		Rok **2030**		Rok **2031**		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. sekcja 1.6)						**OGÓŁEM**	
	PRODUKT																	
	Rodzaj[17]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt całkowity

[17] Produkty odnoszą się do produktów i usług, które mają zostać zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

CEL SZCZEGÓŁOWY nr 1[18]																				
- Produkt																				
- Produkt																				
- Produkt																				
Cel szczegółowy nr 1 – suma cząstkowa																				
CEL SZCZEGÓŁOWY nr 2																				
- Produkt																				
Cel szczegółowy nr 2 – suma cząstkowa																				
OGÓŁEM																				

[18] Zgodnie z opisem w sekcji 1.3.2. „Cel(e) szczegółowy(-e)”.

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ✠ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej

3.2.3.1. Środki z uchwalonego budżetu

ZATWIERDZONE ŚRODKI	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**OGÓŁEM 2028–2034**
DZIAŁ 4								
Zasoby ludzkie	2,020	2,020	2,020	2,020	2,020	2,020	2,020	**14,140**
Pozostałe wydatki administracyjne	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa DZIAŁ 4	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**14,140**
Poza DZIAŁEM 4								
Zasoby ludzkie	0,525	0,525	0,525	0,525	0,525	0,525	0,525	**3,675**
Pozostałe wydatki o charakterze administracyjnym	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa poza DZIAŁEM 4	**0,525**	**0,525**	**0,525**	**0,525**	**0,525**	**0,525**	**0,525**	**3,675**
OGÓŁEM	**2,545**	**2,545**	**2,545**	**2,545**	**2,545**	**2,545**	**2,545**	**17,815**

3.2.3.2. Środki z zewnętrznych dochodów przeznaczonych na określony cel

ZEWNĘTRZNE DOCHODY PRZEZNACZONE NA OKREŚLONY CEL	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**OGÓŁEM 2028–2034**
DZIAŁ 4								
Zasoby ludzkie	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Pozostałe wydatki administracyjne	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa DZIAŁ 4	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**	**0,000**
Poza DZIAŁEM 4								
Zasoby ludzkie	10,175	10,175	10,175	10,175	10,175	10,175	10,175	**71,228**
Pozostałe wydatki o charakterze administracyjnym	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa poza DZIAŁEM 4	**10,175**	**10,175**	**10,175**	**10,175**	**10,175**	**10,175**	**10,175**	**71,228**
OGÓŁEM	**10,175**	**10,175**	**10,175**	**10,175**	**10,175**	**10,175**	**10,175**	**71,228**

3.2.3.3. Ogółem środki

OGÓŁEM ZATWIERDZONE ŚRODKI + ZEWNĘTRZNE DOCHODY PRZEZNACZONE NA OKREŚLONY CEL	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**OGÓŁEM 2028–2034**

			DZIAŁ 4					
Zasoby ludzkie	2,020	2,020	2,020	2,020	2,020	2,020	2,020	**14,140**
Pozostałe wydatki administracyjne	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa DZIAŁ 4	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**2,020**	**14,140**
Poza DZIAŁEM 4								
Zasoby ludzkie	10,700	10,700	10,700	10,700	10,700	10,700	10,700	**74,903**
Pozostałe wydatki o charakterze administracyjnym	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Suma cząstkowa poza DZIAŁEM 4	**10,700**	**10,700**	**10,700**	**10,700**	**10,700**	**10,700**	**10,700**	**77,903**
OGÓŁEM	**12,720**	**12,720**	**12,720**	**12,720**	**12,720**	**12,720**	**12,720**	**89,043**

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną częściowo pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach DG, uzupełnionych wszelkimi dodatkowymi zasobami, które zostaną pokryte z opłaty przewidzianej w akcie o usługach cyfrowych jako zewnętrzne dochody przeznaczone na określony cel, przy ograniczonym wykorzystaniu budżetu administracyjnego.

3.2.4. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej

3.2.4.1. Finansowane z uchwalonego budżetu

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy (EPC)[19]

ZATWIERDZONE ŚRODKI	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)							
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)	5	5	5	5	5	5	5
20 01 02 03 (w delegaturach UE)	0	0	0	0	0	0	0
(Pośrednie badania naukowe)	0	0	0	0	0	0	0
(Bezpośrednie badania naukowe)	0	0	0	0	0	0	0
Inna linia budżetowa (określić)	0	0	0	0	0	0	0
• Personel zewnętrzny (w EPC)							
20 02 01 (CA, SNE z globalnej koperty finansowej)	10	10	10	10	10	10	10

[19] Proszę określić w tabeli poniżej, ile EPC w ramach wskazanej liczby jest już przydzielonych na zarządzanie tym działaniem lub może zostać przesuniętych w ramach Państwa dyrekcji generalnej oraz jakie są Państwa potrzeby netto.

20 02 03 (CA, LA, SNE i JPD w delegaturach UE)		0	0	0	0	0	0	0
Linia budżetowa na wsparcie administracyjne	• w centrali	0	0	0	0	0	0	0
[XX.01.YY.YY]	• w delegaturach UE	0	0	0	0	0	0	0
(CA, SNE – pośrednie badania naukowe)		0	0	0	0	0	0	0
(CA, SNE – bezpośrednie badania naukowe)		0	0	0	0	0	0	0
Inna linia budżetowa (określić) – dział 4		0	0	0	0	0	0	0
Inne linie budżetowe (Urząd ds. AI) – poza działem 4		5	5	5	5	5	5	5
OGÓŁEM		**20**	**20**	**20**	**20**	**20**	**20**	**20**

3.2.4.2. Finansowane z zewnętrznych dochodów przeznaczonych na określony cel

ZEWNĘTRZNE DOCHODY PRZEZNACZONE NA OKREŚLONY CEL		Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)		0	0	0	0	0	0	0
20 01 02 03 (w delegaturach UE)		0	0	0	0	0	0	0
(Pośrednie badania naukowe)		0	0	0	0	0	0	0
(Bezpośrednie badania naukowe)		0	0	0	0	0	0	0
Inne linie budżetowe (opłata przewidziana w akcie o usługach cyfrowych)		15	15	15	15	15	15	15
• Personel zewnętrzny (w EPC)								
20 02 01 (CA, SNE z globalnej koperty finansowej)		0	0	0	0	0	0	0
20 02 03 (CA, LA, SNE i JPD w delegaturach UE)		0	0	0	0	0	0	0
Linia budżetowa na wsparcie administracyjne	• w centrali	0	0	0	0	0	0	0
[XX.01.YY.YY]	• w delegaturach UE	0	0	0	0	0	0	0
(CA, SNE – pośrednie badania naukowe)		0	0	0	0	0	0	0
(CA, SNE – bezpośrednie badania naukowe)		0	0	0	0	0	0	0
Inna linia budżetowa (określić) – dział 4		0	0	0	0	0	0	0
Inne linie budżetowe (opłata przewidziana w akcie o usługach cyfrowych) – poza działem 4		50	50	50	50	50	50	50
OGÓŁEM		**65**	**65**	**65**	**65**	**65**	**65**	**65**

3.2.4.3. Zapotrzebowanie na zasoby ludzkie ogółem

OGÓŁEM ZATWIERDZONE ŚRODKI + ZEWNĘTRZNE DOCHODY PRZEZNACZONE NA OKREŚLONY CEL	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)							
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)	5	5	5	5	5	5	5
20 01 02 03 (w delegaturach UE)	0	0	0	0	0	0	0
(Pośrednie badania naukowe)	0	0	0	0	0	0	0
(Bezpośrednie badania naukowe)	0	0	0	0	0	0	0
Inne linie budżetowe (opłata przewidziana w akcie o usługach cyfrowych)	15	15	15	15	15	15	15
• Personel zewnętrzny (w EPC)							
20 02 01 (CA, SNE z globalnej koperty finansowej)	10	10	10	10	10	10	10
20 02 03 (CA, LA, SNE i JPD w delegaturach UE)	0	0	0	0	0	0	0
Linia budżetowa na wsparcie administracyjne • w centrali	0	0	0	0	0	0	0
[XX.01.YY.YY] • w delegaturach UE	0	0	0	0	0	0	0
(CA, SNE – pośrednie badania naukowe)	0	0	0	0	0	0	0
(CA, SNE – bezpośrednie badania naukowe)	0	0	0	0	0	0	0
Inna linia budżetowa (określić) – dział 4	0	0	0	0	0	0	0
Inne linie budżetowe (segment EFK dotyczący technologii cyfrowych – linia budżetowa na wsparcie administracyjne i opłata przewidziana w akcie o usługach cyfrowych) – poza działem 4	55	55	55	55	55	55	55
OGÓŁEM	**85**	**85**	**85**	**85**	**85**	**85**	**85**

Ewentualne wewnętrzne przesunięcia w ramach Komisji są z należycie uzasadnionych powodów niewystarczające. Wniosek wymaga zatem dodatkowych zasobów ludzkich w DG CONNECT. Finansowanie tych dodatkowych zasobów będzie pochodzić głównie z opłaty przewidzianej w akcie o usługach cyfrowych jako zewnętrznych dochodów przeznaczonych na określony cel, przy ograniczonym wykorzystaniu budżetu administracyjnego.

Personel niezbędny do wdrożenia wniosku (w EPC):

	Przeniesiony wewnętrznie		**Personel dodatkowy**		
	W ramach wdrażających dyrekcji generalnych*	**Wyjątkowo z puli przeniesień Komisji po**	**Finansowany z działu 7***/„Badania naukowe”	**Finansowany z linii BA**	**Finansowany z opłat**

		uzyskaniu informacji od CMB**			
Stanowiska w planie zatrudnienia	5				15
Personel zewnętrzny (CA, SNE, INT)	35 (finansowane już z opłaty przewidzianej w akcie o usługach cyfrowych) 5 (Urząd ds. AI)	10			15
Ogółem	45	10			30

Skala, znaczenie i wymagana szybkość nowych zadań nadzorczych powierzonych Komisji Europejskiej wykraczają poza to, co można pokryć z istniejących zasobów ludzkich i wewnętrznych przesunięć w Komisji.

W porównaniu z istniejącymi ramami egzekwowania przepisów na podstawie aktu o usługach cyfrowych i aktu w sprawie AI instrument ten powierza Komisji szereg nowych zadań nadzorczych – głównie egzekwowanie odroczonego dostępu małoletnich do usług sieci społecznościowych i usług platformy udostępniania wideo, ale również istotne elementy, takie jak nadzór nad wymogami uwzględniania bezpieczeństwa na etapie projektowania, które mają zostać wdrożone przez dostawców internetowych usług sieci społecznościowych, usług platformy udostępniania wideo, a także przez dostawców towarzyszy AI i ogólnych chatbotów konwersacyjnych, w przypadku gdy usługi te są objęte nadzorem Komisji.

Egzekwowanie tych nowych przepisów ma wyjątkowo duże znaczenie społeczne, ponieważ mają one na celu ochronę jednych z najsłabszych członków społeczeństwa: dzieci. Odpowiednie dowody wskazują na znaczne zagrożenia rozwojowe i zdrowotne, na które podatne są dzieci w internecie. Zagrożenia te wymagają nowych przepisów i sprawiają, że egzekwowanie tych przepisów staje się zadaniem o najwyższym znaczeniu społecznym. Oczekiwania polityczne i społeczne, w tym ze strony państw członkowskich, dotyczące skutecznego nadzoru i egzekwowania przepisów w celu ochrony małoletnich w internecie są wysokie, a Komisja będzie musiała w przekonujący sposób wykazać, że jest w stanie ukrócić szkodliwe zachowania.

Ze względu na zwiększone ryzyko, na jakie narażone są dzieci w internecie, instrument ten przewiduje przyspieszoną ścieżkę egzekwowania przepisów, która wymaga od Komisji przyjęcia wstępnych ustaleń w ciągu 30 dni roboczych i podjęcia ostatecznej decyzji w ciągu 90 dni roboczych. Te ramy czasowe egzekwowania przepisów są bezprecedensowe. Komisja będzie zobowiązana do egzekwowania nowych przepisów tego instrumentu nie tylko w trybie przyspieszonym, ale również wobec największych i najbardziej zasobnych przedsiębiorstw na świecie, w środowisku, w którym często dochodzi do sporów sądowych.

Łącznie czynniki te uniemożliwiają poleganie wyłącznie na istniejących zasobach ludzkich i wewnętrznych przesunięciach kadrowych.

Wnioskowany dodatkowy personel doprowadziłby do zwiększenia zatwierdzonych poziomów zatrudnienia na podstawie aktu o usługach cyfrowych o 30 EPC (15 stałych i 15 tymczasowych), finansowanych z opłaty z tytułu aktu o usługach cyfrowych (zewnętrzne dochody przeznaczone na określony cel). Ponadto w ramach Komisji przesunięto by 10 EPC pracowników niezatrudnionych na stałe, aby zwiększyć poziom zatrudnienia w Urzędzie ds. AI.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	• Bieżące monitorowanie, nadzór i dozór nad VLOPSE lub towarzyszami AI i chatbotami podlegającymi nadzorowi Komisji, obejmujące w szczególności następujące kwestie: • Monitorowanie zachowania dostawców, włącznie z regularną i ciągłą analizą, w tym przegląd sprawozdań dotyczących skuteczności środków, regularny przegląd dokumentów dotyczących przejrzystości sporządzonych za pośrednictwem aktu o usługach cyfrowych lub nowego instrumentu, np. sprawozdań z przejrzystości, ocen ryzyka, wniosków o dostęp do danych itp. oraz wniosków o dostęp do danych/algorytmów, testowanie i wsparcie analizy. • Ciągłe prace nad potwierdzaniem wieku, w tym dalsze prace nad unijnym planem weryfikacji wieku i unijnym systemem weryfikacji wieku, ocena alternatywnych rozwiązań z zakresu weryfikacji wieku i rozwiązań w zakresie potwierdzania wieku, prace nad standardami technicznymi, współpraca z państwami członkowskimi w zakresie architektury tożsamości i poświadczeń oraz rozwój zarządzania zaufanymi dostawcami i stronami ufającymi. • Wdrożenie unijnego systemu weryfikacji wieku, w tym ocena zgodności kandydatów na dostawców unijnych rozwiązań z zakresu weryfikacji wieku i kandydatów na dostawców unijnych poświadczeń dowodu wieku oraz zarządzanie związaną z tym infrastrukturą. • Współpraca z koordynatorami ds. usług cyfrowych / organami nadzoru rynku, Radą ds. Usług Cyfrowych lub Radą ds. AI i centrami bezpieczniejszego internetu. • Obsługa całodobowego centrum kryzysowego. • Badania naukowe i prognozowanie, aby na bieżąco śledzić szybko zachodzące zmiany i mieć świadomość zmieniających się skutków dla społeczeństwa, np. związanych z małoletnimi i zdrowiem. • Postępowanie egzekucyjne i nadzór nad środkami zaradczymi: • Przyspieszone procedury podejmowania szybkich działań w przypadku nieprzestrzegania przepisów, w tym wykonywanie czynności dochodzeniowych, takich jak wnioski o udzielenie informacji, wywiady, analiza algorytmów, inspekcje, analiza zobowiązań, ocena planów działania. • Współpraca z koordynatorami ds. usług cyfrowych / organami nadzoru rynku w zakresie czynności dochodzeniowych, np. współpraca z koordynatorami ds. usług cyfrowych / organami nadzoru rynku w zakresie dochodzeń, ocena uzasadnionych wniosków o podjęcie działań przez koordynatorów ds. usług cyfrowych / organy nadzoru rynku, konsultacje/wymiana informacji w ramach Rady. • Wspieranie ogólnej współpracy transgranicznej i egzekwowania przepisów, w tym: • Ocena działań koordynatorów ds. usług cyfrowych / organów nadzoru rynku w zakresie usług/systemów wchodzących w zakres ich obowiązków. • Wsparcie dla Rady, w tym przygotowanie porządku obrad, organizacja grup

	roboczych i sporządzanie projektów dokumentów. • Inne środki regulacyjne. • Przyjmowanie aktów delegowanych i wykonawczych oraz dokumentów zawierających wytyczne (w tym dodatkowych aktów/wytycznych wymaganych w sprawozdaniu PE); • Kodeksy postępowania i certyfikacja. • Środki wspierające. • Wspieranie państw członkowskich w promowaniu i podejmowaniu działań na rzecz rozwoju umiejętności cyfrowych oraz rozwoju kanałów pomocy, zgodnie z art. 32 nowego instrumentu ustawodawczego. • Ułatwianie wymiany najlepszych praktyk, w tym w zakresie rozwoju umiejętności cyfrowych, krajowych kanałów wsparcia i aplikacji, oraz wydawanie wytycznych. • Międzynarodowe działania informacyjne i interakcje z organami regulacyjnymi / organami egzekwowania prawa państw trzecich.
Personel zewnętrzny	• Udział w zarządzaniu działaniami związanymi z wdrażaniem i egzekwowaniem przepisów. • Wspieranie zadań związanych z dokumentami w celu wsparcia zespołów zajmujących się sprawami, w tym poprzez zapewnienie należytego składania dokumentów i spójności z zasadami proceduralnymi i terminami. • Przygotowywanie korespondencji z nadzorowanymi podmiotami oraz dostępu do akt spraw. • Podstawowe badania i analizy.

3.2.5. Przegląd szacowanego wpływu na inwestycje związane z technologiami cyfrowymi

Obowiązkowo w tabeli poniżej: szacowany wpływ wniosku/inicjatywy na inwestycje związane z technologiami cyfrowymi.

W wyjątkowych przypadkach, jeżeli wymaga tego realizacja wniosku/inicjatywy, we wskazanym wierszu należy podać środki z działu 4.

Środki z działów 1–3 należy podać w wierszu „Wydatki na IT wynikające z realizacji polityki tytułem programów operacyjnych”. Wydatki te odnoszą się do budżetu operacyjnego na ponowne wykorzystanie / zakup / rozwój platform / narzędzi informatycznych bezpośrednio związanych z realizacją inicjatywy oraz powiązanych z nimi inwestycji (np. licencje, badania, przechowywanie danych). Informacje podane w tej tabeli powinny zgadzać się z informacjami przedstawionymi w sekcji 4 „Wymiar cyfrowy”.

OGÓŁEM środki na IT i technologie cyfrowe	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	**OGÓŁEM WRF 2028–2034**
DZIAŁ 4								
Wydatki na IT (ponoszone przez organizację)	0	0	0	0	0	0	0	**0**
Suma cząstkowa DZIAŁ 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Poza DZIAŁEM 4								
Wydatki na IT wynikające z realizacji polityki tytułem programów operacyjnych	0	0	0	0	0	0	0	**0**
Suma cząstkowa poza DZIAŁEM 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
OGÓŁEM	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

– ☐ może zostać w pełni sfinansowany(-a) przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF)

– ☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF

– ☐ wymaga rewizji WRF

3.2.7. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

– ☒ nie przewiduje współfinansowania ze strony osób trzecich

– ☐ przewiduje współfinansowanie ze strony osób trzecich zgodnie z poniższymi szacunkami:

środki w mln EUR (do trzech miejsc po przecinku)

	Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**	Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

3.3. Szacunkowy wpływ na dochody

– ☐ Wniosek/inicjatywa nie ma wpływu finansowego na dochody

– ☒ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

  – ☐ wpływ na zasoby własne

  – ☒ wpływ na inne dochody (przeznaczone na określony cel)

– ☐ Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[20]						
		Rok **2028**	Rok **2029**	Rok **2030**	Rok **2031**	Rok **2032**	Rok **2033**	Rok **2034**
02 20 03 05		17,875	15,875	15,875	15,875	15,875	15,875	15,875

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

02 20 03 05 Akt o usługach cyfrowych – Nadzór nad bardzo dużymi platformami internetowymi Inne uwagi (np. metoda/wzór stosowane do obliczania wpływu na dochody lub wszelkie inne informacje).

4. WYMIAR CYFROWY

Aby zapewnić zgodność z niniejszym rozporządzeniem, dostawcy usług i systemów cyfrowych objęci jego zakresem muszą ustalić wiek odbiorców usługi lub użytkownika systemu zgodnie z wymogami ustanowionymi w rozdziale V. Wdrożenie „odroczenia dostępu” wymaga od dostawców usług sieci społecznościowych lub usług platform udostępniania wideo w szczególności stosowania solidnych i skutecznych unijnych rozwiązań z zakresu weryfikacji wieku, opartych na unijnym planie weryfikacji wieku udostępnionym przez Komisję. Państwa członkowskie lub podmioty prywatne mogą korzystać z takiego rozwiązania jako samodzielnej aplikacji lub jako części portfela cyfrowego. Rozwiązanie to jest przyjazne dla użytkownika, bezpieczne i w pełni chroniące prywatność. Do celów realizacji obowiązków w zakresie uwzględniania bezpieczeństwa na etapie projektowania rozwiązania w zakresie potwierdzania wieku, inne niż unijna weryfikacja wieku, mogą być również stosowane w celu zapewnienia zgodności z rozporządzeniem, pod warunkiem że spełniają określone kryteria. Aby działanie to było skuteczne w praktyce, ważne jest, aby istniały rozwiązania w zakresie weryfikacji wieku i rozwiązania w zakresie potwierdzania wieku, które zapewniają wysoki poziom dokładności, wiarygodności, bezpieczeństwa, odporności, nieinwazyjności, ochrony prywatności i danych oraz niedyskryminacji. Na rynku dostępne są już rozwiązania komercyjne pozwalające określić wiek usługobiorcy, z których można korzystać zgodnie z przepisami niniejszego rozporządzenia, pod warunkiem że zapewniają one wystarczający poziom ochrony.

Ponadto w następstwie zalecenia Komisji (UE) 2026/1035 Komisja opracowuje unijny system weryfikacji wieku, który obejmuje wymogi dotyczące modelu zaufania, zarządzania oraz wymagań, które muszą spełniać dostawcy poświadczeń

[20] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 10 % na poczet kosztów poboru, zgodnie z propozycją zawartą w COM(2025)574.

dowodu wieku i rozwiązań z zakresu weryfikacji wieku. Podmioty powinny spełnić wymogi unijnego systemu weryfikacji wieku, zanim ich rozwiązania oraz dostawców poświadczeń dowodu wieku będzie można dodać, odpowiednio, do unijnej listy zaufanych rozwiązań. Podobnie dostawcy poświadczeń dowodu wieku powinni spełnić wymogi unijnego systemu weryfikacji wieku, zanim będą mogli zostać dodani do unijnej listy zaufanych dostawców poświadczeń dowodu wieku. Unijny system weryfikacji wieku będzie wymagał wsparcia w zakresie jego utrzymania i funkcjonowania w perspektywie średnio- i długoterminowej.

4.1. Wymogi cyfrowe

W tym kontekście w rozporządzeniu ustanowiono następujące wymogi:

Wymóg 1 (R1): dostawcy usług, w przypadku których dostęp zostaje odroczony, są zobowiązani do zaproponowania odbiorcom swoich usług i użytkownikom systemów potwierdzenia wieku za pomocą unijnych rozwiązań z zakresu weryfikacji wieku korzystających z unijnego poświadczenia dowodu wieku lub innych rozwiązań, o których mowa w art. 24 ust. 2 lit. a) i b) niniejszego rozporządzenia.

Wymóg 2 (R2): dostawcy podlegający obowiązkom uwzględniania bezpieczeństwa na etapie projektowania oraz dostawcy sklepów z aplikacjami mogą korzystać z rozwiązań w zakresie potwierdzania wieku innych niż unijne rozwiązania z zakresu weryfikacji wieku, pod warunkiem że zapewniają one wysoki poziom dokładności, niezawodności, bezpieczeństwa, odporności, nieinwazyjności, ochrony prywatności i danych oraz niedyskryminacji.

Wymóg 3 (R3): Komisja Europejska przyjmuje akty wykonawcze obejmujące istniejące specyfikacje i funkcjonowanie unijnego systemu weryfikacji wieku, a także wykaz podmiotów wydających unijne poświadczenia dowodu wieku oraz wykaz unijnych rozwiązań z zakresu weryfikacji wieku.

Jak wspomniano powyżej, do celów R1 i R2 Komisja opracowała już unijny plan weryfikacji wieku, który obecnie wymaga przyjęcia przez państwa członkowskie lub przedsiębiorstwa prywatne. Do celów R3 Komisja ustanawia już unijny system weryfikacji wieku oraz dwie listy.

Do celów wymiany informacji między odpowiedzialnymi organami wykorzystywany będzie system AGORA, który jest bezpiecznym systemem wymiany informacji wspierającym komunikację między koordynatorami ds. usług cyfrowych w państwach członkowskich, Komisją i Europejską Radą ds. Usług Cyfrowych (składającą się z koordynatora ds. usług cyfrowych). Komisja, koordynatorzy ds. usług cyfrowych i Rada korzystają z systemu AGORA we wszelkiej komunikacji związanej z egzekwowaniem aktu o usługach cyfrowych. System ten został już ustanowiony i będzie teraz wykorzystywany również do celów niniejszego rozporządzenia, co potencjalnie wymagałoby dalszego włączenia organów do systemu, chociaż takie dodatkowe włączenie jest prawdopodobnie ograniczone, ponieważ odpowiednie organy zostały już w większości włączone. W związku z tym kwestia ta nie zostanie poruszona w niniejszej ocenie skutków finansowych i cyfrowych regulacji. To samo dotyczy nadzoru i egzekwowania przepisów w odniesieniu do towarzyszy AI i chatbotów, które będą opierać się na strukturach, ramach egzekwowania przepisów i systemie wymiany informacji ustanowionym już na mocy aktu w sprawie sztucznej inteligencji.

4.2. Dane

Unijne rozwiązanie z zakresu weryfikacji wieku jest rozwiązaniem, które chroni prywatność, minimalizuje dane, nie jest identyfikowalne ani możliwe do powiązania i jest „podwójnie ślepe" oraz zaprojektowane w taki sposób, aby przetwarzanie danych osobowych było ograniczone do bezwzględnie niezbędnego minimum. W wielu przypadkach wiek danej osoby można zweryfikować na podstawie istniejących danych, którymi dysponuje dostawca poświadczeń dowodu wieku. Przedstawienie poświadczenia dowodu wieku wiąże się z przetwarzaniem danych osobowych osób, które muszą udowodnić swój wiek za pomocą usług online. Takie przetwarzanie danych odbywa się niezależnie od dostępu danej osoby do takich usług online. Sama usługa online nie otrzymuje żadnych danych osobowych użytkownika w wyniku procesu weryfikacji wieku, z wyjątkiem dowodu, że dana osoba przekroczyła wymagany wiek. Przetwarzanie danych w pełni chroni prywatność i wykorzystuje najnowsze technologie w celu zapewnienia pełnej zgodności ze standardami ochrony danych. Technologia ta jest regularnie aktualizowana, aby zachować jej bezpieczny i chroniący prywatność charakter. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

4.3. Rozwiązania cyfrowe

Unijny system weryfikacji wieku to zestaw wymogów technicznych opartych na otwartym oprogramowaniu, które można wykorzystać do opublikowania samodzielnej mobilnej aplikacji do weryfikacji wieku. Zarówno państwa członkowskie, jak i podmioty prywatne mogą opracować rozwiązanie z zakresu weryfikacji wieku.

Rozwiązanie to umożliwia osobom fizycznym udowodnienie w ramach usług i systemów cyfrowych wymagających weryfikacji wieku, że ich wiek jest wystarczający, bez ujawniania swojej tożsamości, dokładnego wieku, daty urodzenia lub innych danych osobowych. To rozwiązanie cyfrowe wspiera wymogi cyfrowe R1 i R2 i jest pośrednio powiązane z R3, ponieważ dostarcza poświadczenia dowodu wieku potwierdzające, że osoby fizyczne osiągnęły (lub nie) określony wiek.

4.4. Ocena interoperacyjności

Europejskie rozwiązanie w zakresu weryfikacji wieku jest zgodne pod względem technicznym z europejskimi portfelami tożsamości cyfrowej określonymi w rozporządzeniu (UE) nr 910//2014 ustanawiającym europejskie ramy tożsamości cyfrowej. Poświadczenie dowodu wieku będzie wydawane jako elektroniczne poświadczenie atrybutów, jak określono w art. 3 pkt 44 rozporządzenia (UE) nr 910/2014. Gwarantuje to, że rozwiązania z zakresu weryfikacji wieku i dostawcy poświadczeń dowodu wieku będą dostarczać (potencjalnym) odbiorcom usługi poświadczenia wieku, które mogą być wykorzystywane w usługach cyfrowych i we wszystkich państwach członkowskich.

Podstawowa specyfika rozwiązań z zakresu weryfikacji wieku umożliwia zatem niezakłóconą interoperacyjność usług cyfrowych dla potencjalnych odbiorców usług cyfrowych w celu udowodnienia ich wieku.

4.5. Środki wspierające cyfrowe wdrażanie

Jak wspomniano w sekcji 4.1, Komisja jest już na dobrej drodze do wspierania cyfrowego

wdrażania niniejszego rozporządzenia poprzez publikację planu działania UE i trwające prace nad unijnym systemem weryfikacji wieku. Powinno to umożliwić istnienie infrastruktury i systemu w momencie rozpoczęcia stosowania.

Aby zapewnić absorpcję przez społeczeństwo, ale także umożliwić stałe przekazywanie opinii publicznej informacji zwrotnych i aktualizacji, Komisja Europejska opublikowała wymogi techniczne niezbędne do opracowania unijnych rozwiązań z zakresu weryfikacji wieku. Jest to projekt typu open source, a wszystkie informacje są publicznie dostępne na stronie internetowej ageverification.dev. Ta strona internetowa i związana z nią testowa infrastruktura informatyczna będą wymagały bieżącej konserwacji i eksploatacji. Ponadto trwające prace nad unijnym systemem weryfikacji wieku powinny sprawić, że opracowywanie aktów wykonawczych w celu wsparcia tych prac będzie proste, ponieważ będzie opierać się na istniejącej praktyce. Kluczowe znaczenie będą miały kampanie podnoszące świadomość w okresie wejścia w życie, nie tylko w celu wspierania szerokiego upowszechnienia wśród społeczeństwa, ale także w celu złagodzenia obaw związanych z prywatnością i użytecznością.