



KOMISJA
EUROPEJSKA

Bruksela, dnia 7.10.2025 r.
C(2025) 6826 final

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**

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

1 WPROWADZENIE

1. Osoby małoletnie mają coraz większy dostęp do platform internetowych ⁽¹⁾ i mogą czerpać z nich szereg korzyści. Platformy internetowe mogą przykładowo zapewniać dostęp do wielu zasobów edukacyjnych, pomagając małoletnim w zdobywaniu nowych umiejętności i poszerzaniu wiedzy. Platformy internetowe mogą również oferować małoletnim możliwość wyrażania poglądów i nawiązywania kontaktów z innymi osobami o podobnych zainteresowaniach, co pomaga w budowaniu umiejętności społecznych, pewności siebie i poczucia wspólnoty. Dzięki zabawie w środowisku internetowym i odkrywaniu go małoletni mogą również rozwijać swoją naturalną ciekawość, angażując się w działania, które zachęcają do kreatywności, rozwiązywania problemów, krytycznego myślenia, bycia sprawczym i zapewniają rozrywkę.
2. Wśród decydentów, organów regulacyjnych, społeczeństwa obywatelskiego, naukowców, pracowników pedagogicznych i opiekunów ⁽²⁾ panuje jednak powszechna zgoda co do tego, że obecny poziom prywatności, bezpieczeństwa i ochrony małoletnich w internecie jest często niewystarczający. Konstrukcja i cechy wielu platform internetowych i usług oferowanych przez dostawców platform internetowych dostępnych dla małoletnich mogą powodować ryzyko w odniesieniu do prywatności, bezpieczeństwa i ochrony małoletnich oraz pogłębiać istniejące zagrożenia. Zagrożenia te to m.in. narażenie na treści nielegalne ⁽³⁾ i szkodliwe, które naruszają prywatność, bezpieczeństwo i ochronę małoletnich lub mogą szkodzić ich rozwojowi fizycznemu bądź psychicznemu. Zalicza się do nich również

⁽¹⁾ W niniejszych wytycznych terminy „dziecko”, „dzieci” i „małoletni” odnoszą się do osoby poniżej 18 roku życia.

⁽²⁾ W niniejszych wytycznych termin „opiekun” odnosi się do osób, na których spoczywa odpowiedzialność rodzicielska.

⁽³⁾ Do nielegalnych treści zalicza się m.in. treści przedstawiające nielegalny obrót środkami odurzającymi, treści terrorystyczne i brutalne treści ekstremistyczne oraz materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych. Nielegalnych treści nie zdefiniowano w rozporządzeniu (UE) 2022/2065 (akt o usługach cyfrowych), lecz w innych przepisach na szczeblu UE lub krajowym.

cyberszykanowanie lub kontakt ze strony osób działających na szkodę małoletnich, np. osób usiłujących wykorzystywać małoletnich seksualnie lub dopuszczać się wobec nich szantażu przy użyciu treści pornograficznych, handlarzy ludźmi oraz osób próbujących zwerbować małoletnich do grup przestępczych lub propagujących przemoc, radykalizację, brutalny ekstremizm i terroryzm. Małoletni mogą również napotykać ryzyko jako konsumenci, a także zagrożenia związane z powszechnym lub nadmiernym korzystaniem z platform internetowych oraz narażeniem na niewłaściwe lub oparte na wyzysku praktyki, w tym w odniesieniu do hazardu i gier. Coraz szersze włączanie do platform internetowych chatbotów i asystentów opartych na sztucznej inteligencji („AI”), a także wytworzone za pomocą AI materiały deepfake mogą również wpływać na sposób interakcji małoletnich z platformami internetowymi, pogłębiać istniejące zagrożenia i stwarzać nowe, potencjalnie wywierające negatywny wpływ na prywatność, bezpieczeństwo i ochronę małoletniego ⁽⁴⁾. Zagrożenia te mogą wynikać z bezpośredniego kontaktu małoletniego z platformą lub z działań innych użytkowników platformy.

3. Niniejsze wytyczne mają wspierać dostawców platform internetowych w przeciwdziałaniu temu ryzyku dzięki przedstawieniu zbioru środków, które zdaniem Komisji pomogą im zapewnić na ich platformach wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich, co przyczyni się do realizacji ważnego celu polityki Unii, jakim jest ochrona małoletnich. Niniejsze wytyczne mają również pomóc koordynatorom ds. usług cyfrowych i właściwym organom krajowym w stosowaniu i interpretacji art. 28 rozporządzenia (UE) 2022/2065. Na przykład zwiększenie poziomu prywatności kont małoletnich pomoże m.in. dostawcom platform internetowych zmniejszyć ryzyko niepożądanego lub nieproszonego kontaktu. Wdrożenie środków potwierdzania wieku ⁽⁵⁾ może m.in. pomóc dostawcom ograniczyć ryzyko narażenia małoletnich na usługi, treści, zachowania, kontakty lub praktyki handlowe, które naruszają ich prywatność, bezpieczeństwo i ochronę. Przyjęcie tych i innych środków – od systemów rekomendacji i zarządzania po wsparcie użytkownika i zgłoszenia – może pomóc dostawcom platform

⁽⁴⁾ Typologię ryzyka, na które narażone są małoletni podczas korzystania z platform internetowych, opartą na ramach opracowanych przez OECD, przedstawiono w załączniku I do niniejszych wytycznych.

⁽⁵⁾ Zob. sekcja 6.1 dotycząca potwierdzania wieku.

internetowych w zwiększeniu bezpieczeństwa, ochrony i prywatności małoletnich na tych platformach.

2 ZAKRES WYTYCZNYCH

4. Właśnie ze względu na wyżej wymienione czynniki ryzyka prawodawca Unii przyjął art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 ⁽⁶⁾. W ust. 1 wspomnianego przepisu 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 art. 28 ust. 2 rozporządzenia (UE) 2022/2065 zakazuje się dostawcom platform internetowych prezentowania w swoim interfejsie reklam opartych na profilowaniu zgodnie z definicją zawartą w art. 4 pkt 4 rozporządzenia (UE) 2016/679 ⁽⁷⁾ z wykorzystaniem danych osobowych odbiorcy usługi, jeżeli wiedzą z wystarczającą pewnością, że odbiorca usługi jest małoletni. Art. 28 ust. 3 rozporządzenia (UE) 2022/2065 stanowi, że wypełnianie obowiązków określonych w tym artykule nie zobowiązuje dostawców platform internetowych dostępnych dla małoletnich do przetwarzania dodatkowych danych osobowych w celu oceny, czy odbiorca usługi jest małoletni. Art. 28 ust. 4 rozporządzenia (UE) 2022/2065 stanowi, że Komisja, po konsultacji z Europejską Radą ds. Usług Cyfrowych („Rada”), może wydać wytyczne w celu wsparcia dostawców platform internetowych w stosowaniu ust. 1.
5. W niniejszych wytycznych opisano środki, które zdaniem Komisji dostawcy platform internetowych dostępnych dla małoletnich powinni wprowadzić, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w internecie zgodnie z art. 28 ust. 1 rozporządzenia (UE) 2022/2065. Obowiązek ustanowiony w tym przepisie dotyczy dostawców platform internetowych, których usługi są dostępne dla małoletnich ⁽⁸⁾. W motywie 71 wspomnianego rozporządzenia

⁽⁶⁾ 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.

⁽⁷⁾ Rozporządzenie (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), Dz.U. L 119 z 4.5.2016, s. 1.

⁽⁸⁾ Zgodnie z art. 3 rozporządzenia (UE) 2022/2065 „platforma internetowa” oznacza usługę hostingu, która na żądanie odbiorcy usługi przechowuje i rozpowszechnia publicznie informacje, chyba że takie

wyjaśniono ponadto, że „platformę internetową można uznać za dostępną dla małoletnich, jeżeli warunki korzystania z jej usług umożliwiają małoletnim korzystanie z usługi, gdy jej usługa jest skierowana do małoletnich lub korzystają z niej w przeważającej mierze małoletni, lub gdy dostawca w inny sposób ma świadomość, że niektórzy odbiorcy jego usługi są małoletni”.

6. W odniesieniu do pierwszego scenariusza opisanego w tym motywie Komisja uważa, że twierdzenie dostawcy platformy internetowej, iż platforma ta jest niedostępna dla małoletnich, nie może opierać się wyłącznie na zawartym w warunkach korzystania z usług zapisie zakazującym dostępu małoletnim. Jeżeli dostawca platformy internetowej nie wdroży skutecznych środków uniemożliwiających małoletnim dostęp do jego usługi, nie może twierdzić, że jego platforma internetowa nie wchodzi w zakres art. 28 ust. 1 rozporządzenia (UE) 2022/2065 ze względu na taki zapis. Np. w przypadku dostawców platform internetowych, które służą do przechowywania i rozpowszechniania treści dla dorosłych, takich jak platformy internetowe rozpowszechniające treści pornograficzne, i w związku z tym w swoich warunkach korzystania z usług zastrzegają dostęp tylko dla użytkowników w wieku powyżej 18 lat, platformy takie będą uważane za dostępne dla małoletnich w rozumieniu art. 28 ust. 1 rozporządzenia (UE) 2022/2065, jeżeli nie wprowadzono skutecznych środków uniemożliwiających małoletnim dostęp do usług tych platform.
7. Jeżeli chodzi o trzeci scenariusz, w motywie 71 rozporządzenia (UE) 2022/2065 jako jeden z przykładów sytuacji, w której dostawca platformy internetowej powinien mieć świadomość, że niektórzy odbiorcy jej usługi są małoletni, podano sytuację, w której dostawca ten przetwarza już dane osobowe tych odbiorców ujawniające ich wiek do innych celów, np. podczas rejestracji w danej usłudze, w wyniku czego wiadomo, że niektórzy z tych odbiorców są małoletni. Inne przykłady sytuacji, w których można zasadnie oczekiwać od dostawcy świadomości, że wśród odbiorców jego usługi znajdują się małoletni, to sytuacje, w których wiadomo, że platforma internetowa cieszy się zainteresowaniem małoletnich; dostawca platformy internetowej oferuje usługi podobne do tych, z których korzystają małoletni; platforma internetowa jest promowana wśród małoletnich; dostawca platformy

działanie jest nieznaczną lub wyłącznie poboczną cechą innej usługi lub nieznaczną funkcją głównej usługi, i ze względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi, a włączenie takiej cechy lub funkcji w taką inną usługę nie jest sposobem na obejście stosowania [tego] rozporządzenia.

internetowej przeprowadził lub zlecił badanie, w ramach którego zidentyfikowano małoletnich jako odbiorców tych usług lub stwierdzono to w niezależnych badaniach.

8. Zgodnie z art. 19 rozporządzenia (UE) 2022/2065 obowiązek ustanowiony w art. 28 ust. 1 rozporządzenia (UE) 2022/2065 nie ma zastosowania do dostawców platform internetowych, które kwalifikują się jako mikroprzedsiębiorstwa lub małe przedsiębiorstwa, chyba że Komisja wskazała ich platformę jako bardzo dużą platformę internetową zgodnie z art. 33 ust. 4 tego rozporządzenia ⁽⁹⁾.
9. Zapewnieniu ochrony małoletnich w internecie służą również inne przepisy rozporządzenia (UE) 2022/2065 ⁽¹⁰⁾. Należy do nich m.in. szereg przepisów zawartych w rozdziale III sekcja 5 rozporządzenia (UE) 2022/2065, w których nakłada się dodatkowe obowiązki na dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych ⁽¹¹⁾. Niniejsze wytyczne nie mają na celu interpretacji tych przepisów, a dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych nie powinni oczekiwać, że przyjęcie opisanych poniżej środków, w części lub w całości, wystarczy do wypełnienia obowiązków wynikających z rozdziału III sekcja 5 rozporządzenia (UE) 2022/2065, ponieważ w przypadku tych dostawców może być konieczne wprowadzenie dodatkowych środków, których nie określono w niniejszych

⁽⁹⁾ W zaleceniu 2003/361/WE małe przedsiębiorstwo definiuje się jako przedsiębiorstwo, które zatrudnia mniej niż 50 pracowników i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 mln EUR. Mikroprzedsiębiorstwo definiuje się jako przedsiębiorstwo zatrudniające mniej niż 10 osób, którego roczny obrót lub roczna suma bilansowa nie przekracza 2 mln EUR. Komisja przypomina w tym względzie motyw 10 rozporządzenia (UE) 2022/2065, w którym stwierdzono, że rozporządzenie (UE) 2022/2065 pozostaje bez uszczerbku dla dyrektywy (UE) 2010/13. Wspomniana dyrektywa nakłada na wszystkich dostawców platform udostępniania wideo, niezależnie od tego, czy uznaje się ich za mikroprzedsiębiorstwa, czy za małe przedsiębiorstwa, obowiązek stworzenia i obsługi systemów weryfikacji wieku użytkowników platformy udostępniania wideo w odniesieniu do treści, które mogą zaszkodzić fizycznemu lub psychicznemu rozwojowi małoletnich.

⁽¹⁰⁾ Dotyczy to obowiązków określonych w następujących przepisach rozporządzenia (UE) 2022/2065: art. 14 w sprawie warunków korzystania z usług, art. 16 i 17 w sprawie mechanizmów zgłaszania i działania oraz uzasadnienia, art. 25 w sprawie projektu i organizacji interfejsów internetowych, art. 15 i 24 w sprawie przejrzystości, art. 26 w sprawie reklam, art. 27 w sprawie systemów rekomendacji oraz art. 44 w sprawie norm.

⁽¹¹⁾ Dotyczy to m.in. następujących przepisów rozporządzenia (UE) 2022/2065: art. 34 i 35 w sprawie oceny ryzyka i zmniejszania ryzyka, art. 38 w sprawie systemów rekomendacji, art. 40 w sprawie dostępu do danych i kontroli danych oraz art. 44 lit. j) w sprawie norm dotyczących ukierunkowanych środków ochrony małoletnich w internecie.

wytycznych, a które są niezbędne do wypełnienia przez nich obowiązków wynikających ze wspomnianych przepisów ⁽¹²⁾.

10. Art. 28 ust. 1 rozporządzenia (UE) 2022/2065 należy również postrzegać w świetle innych unijnych przepisów i niewiążących instrumentów, które mają na celu przeciwdziałanie ryzyku, na jakie narażeni są małoletni w internecie ⁽¹³⁾. Instrumenty te przyczyniają się również do osiągnięcia celu, jakim jest zapewnienie wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w internecie, a tym samym uzupełniają stosowanie art. 28 ust. 1 rozporządzenia (UE) 2022/2065. Niniejszych wytycznych nie należy rozumieć jako stanowiących interpretację lub ograniczenie jakichkolwiek obowiązków wynikających ze tych instrumentów lub z ustawodawstwa państwa członkowskiego. Nadzór nad stosowaniem tych instrumentów i ich egzekwowanie pozostają w wyłącznej gestii właściwych organów w rozumieniu tych ram prawnych. W szczególności, jak wyjaśniono w motywie 10 rozporządzenia (UE) 2022/2065, rozporządzenie to pozostaje bez uszczerbku dla innych aktów prawa Unii regulujących świadczenie usług społeczeństwa informacyjnego w ujęciu ogólnym, regulujących inne aspekty świadczenia usług pośrednich na rynku wewnętrznym lub określających i uzupełniających przepisy zharmonizowane określone w rozporządzeniu (UE) 2022/2065, takich jak dyrektywa 2010/13/UE, a także prawa Unii w dziedzinie ochrony konsumentów i ochrony danych osobowych, w szczególności rozporządzenia (UE) 2016/679.

⁽¹²⁾ Dotyczy to m.in. art. 34 i 35 w sprawie oceny ryzyka i zmniejszania ryzyka, art. 38 w sprawie systemów rekomendacji oraz art. 40 w sprawie dostępu do danych i kontroli danych.

⁽¹³⁾ Podejście to obejmuje strategię na rzecz lepszego internetu dla dzieci (BIK+), dyrektywę 2010/13/UE („dyrektywa o audiowizualnych usługach medialnych”), rozporządzenie (UE) 2024/1689 („akt w sprawie sztucznej inteligencji”), rozporządzenie (UE) 2016/679 („RODO”), dyrektywę 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci, dyrektywę 2005/29/WE dotyczącą nieuczciwych praktyk handlowych, europejski portfel tożsamości cyfrowej oraz krótkoterminowe rozwiązanie służące weryfikacji wieku, przyszły plan działania przeciwko cyberszyskanowaniu, ogólnounijne badanie dotyczące szerszego wpływu mediów społecznościowych na dobrostan, strategię ProtectEU, unijny plan działania na rzecz zwalczania nielegalnego obrotu środkami odurzającymi i przestępczości zorganizowanej, Forum UE ds. Internetu, [strategię UE na rzecz skuteczniejszej walki z niegodziwym traktowaniem dzieci w celach seksualnych](#) oraz strategię UE w zakresie zwalczania handlu ludźmi na lata 2021–2025. Ponadto rozporządzenie (UE) 2022/2065 pozostaje bez uszczerbku dla prawa Unii w dziedzinie ochrony konsumentów i bezpieczeństwa produktów, w tym rozporządzeń (UE) 2017/2394 i (UE) 2019/1020 oraz dyrektyw 2001/95/WE i 2013/11/UE. Dyrektywa 2005/29 dotycząca nieuczciwych praktyk handlowych, w szczególności art. 5–9, również chroni małoletnich, a np. w pkt 28 załącznika I zakazuje się umieszczania w reklamie bezpośredniego wezwania dzieci do nabycia reklamowanych produktów lub do nakłonienia rodziców lub innych osób dorosłych do kupienia im reklamowanych produktów. Komisja przypomina również o przeprowadzonej przez siebie ocenie adekwatności unijnego prawa ochrony konsumentów w zakresie sprawiedliwości cyfrowej.

11. W niniejszych wytycznych określono środki mające na celu zapewnienie wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w internecie, ale dostawców platform internetowych zachęca się do przyjęcia tych środków w celu ochrony wszystkich użytkowników, a nie tylko małoletnich. Stworzenie zapewniającego prywatność, bezpiecznego i chronionego środowiska internetowego dla wszystkich użytkowników siłą rzeczy doprowadzi do zwiększenia prywatności, bezpieczeństwa i ochrony małoletnich w internecie, przy jednoczesnym przyjęciu środków zapewniających poszanowanie ich szczególnych praw i potrzeb zgodnie z art. 28 rozporządzenia (UE) 2022/2065.
12. Przyjmując niniejsze wytyczne, Komisja oświadcza, że będzie stosować je w przypadkach opisanych w niniejszym dokumencie, a tym samym wyznaczy sobie granice wykonywania przysługujących jej uprawnień dyskrejonalnych w każdym przypadku stosowania art. 28 ust. 1 rozporządzenia (UE) 2022/2065. W związku z tym niniejsze wytyczne można uznać za istotny i znaczący punkt odniesienia, który Komisja będzie uwzględniać przy stosowaniu art. 28 ust. 1 rozporządzenia (UE) 2022/2065 i określaniu, czy dostawcy platform internetowych dostępnych dla małoletnich przestrzegają tego przepisu⁽¹⁴⁾. Z niniejszych wytycznych mogą również czerpać inspirację koordynatorzy ds. usług cyfrowych i właściwe organy krajowe przy stosowaniu i interpretacji art. 28 ust. 1 rozporządzenia 2022/2065. Niemniej jednak przyjęcie i wdrożenie środków określonych w niniejszych wytycznych, w części lub w całości, nie oznacza automatycznie zgodności ze wspomnianym przepisem.
13. Wszelkiej autorytatywnej wykładni art. 28 ust. 1 rozporządzenia (UE) 2022/2065 może dokonywać wyłącznie Trybunał Sprawiedliwości Unii Europejskiej, który jest m.in. właściwy do wydawania orzeczeń w trybie prejudycjalnym w przedmiocie ważności i wykładni aktów Unii, w tym art. 28 ust. 1 rozporządzenia (UE) 2022/2065.

⁽¹⁴⁾ Przyjęcie i wdrożenie któregokolwiek ze środków określonych w niniejszych wytycznych nie oznacza zgodności z RODO ani z żadnymi innymi mających zastosowanie przepisami o ochronie danych. Zachęca się zatem odpowiedzialne organy, aby przy ustalaniu zgodności z art. 28 ust. 1 rozporządzenia (UE) 2022/2065 współpracowały z organami ochrony danych.

14. W trakcie opracowywania wytycznych Komisja prowadziła konsultacje z zainteresowanymi stronami ⁽¹⁵⁾, w tym z Radą i jej grupą roboczą ds. ochrony małoletnich. Zgodnie z art. 28 ust. 4 rozporządzenia (UE) 2022/2065 Komisja skonsultowała się z Radą w sprawie projektu niniejszych wytycznych przed ich przyjęciem w dniu 2 lipca 2025 r.
15. Środki opisane w sekcjach 5–8 niniejszych wytycznych nie są wyczerpujące. Za odpowiednie i proporcjonalne w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich zgodnie z art. 28 ust. 1 rozporządzenia (UE) 2022/2065 można uznać również inne środki, np. wynikające z przestrzegania innych przepisów Unii ⁽¹⁶⁾ lub stosowania się do krajowych wytycznych dotyczących ochrony małoletnich bądź norm technicznych ⁽¹⁷⁾. Ponadto w przyszłości można określić nowe środki, które umożliwią dostawcom platform internetowych dostępnych dla małoletnich lepsze wywiązywanie się z obowiązku zapewnienia

⁽¹⁵⁾ Komisja opracowała wytyczne, przeprowadzając szczegółowe badanie źródeł wtórnych oraz gromadząc informacje zwrotne od zainteresowanych stron w drodze zaproszenia do zgłaszania uwag, warsztatów i ukierunkowanych konsultacji publicznych. W trakcie całego procesu Komisja korzystała również z wiedzy fachowej Europejskiego Centrum Przejrzystości Algorytmicznej. Ponadto Komisja skonsultowała się z młodymi ludźmi, w tym z ambasadorami młodzieżowymi inicjatywy „Lepszy internet dla dzieci”, oraz zorganizowała grupy dyskusyjne z dziećmi w siedmiu państwach członkowskich, przy wsparciu centrów bezpieczniejszego internetu.

⁽¹⁶⁾ Dotyczy to np. dyrektyw i rozporządzeń przywołanych w przypisie 13, przyszłych wytycznych Europejskiej Rady Ochrony Danych (EROD) w sprawie przetwarzania danych osobowych osób małoletnich zgodnie z rozporządzeniem (UE) 2016/679 (RODO).

⁽¹⁷⁾ An Coimisiún um Chosaint Sonraí (2021). *Fundamentals for a child-oriented approach to data processing* [Podstawy ukierunkowanego na dzieci podejścia do przetwarzania danych]. Dostępne na stronie: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf; Coimisiún na Meán (2024). *Online safety code* [Kodeks bezpieczeństwa w internecie]. Dostępne na stronie: <https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf>; IMY (Szwedzki Urząd Ochrony Danych) (2021). *The rights of children and young people on digital platforms* [Prawa dzieci i młodzieży na platformach cyfrowych]. Dostępne na stronie: <https://www.imy.se/en/publications/the-rights-of-children-and-young-people-on-digital-platforms/>; Niderlandzkie Ministerstwo Spraw Wewnętrznych i Relacji w Królestwie (2022). *Code for children's rights* [Kodeks praw dziecka]. Dostępne na stronie: <https://codevoorkinderrechten.waag.org/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf>

CNIL (2021). *CNIL publishes 8 recommendations to enhance protection of children online* [CNIL publikuje osiem zaleceń dotyczących poprawy ochrony dzieci w internecie]. Dostępne na stronie: <https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online>; Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs (brak daty). *Rechtsfragen Digitales*. Dostępne na stronie: <https://beauftragte-missbrauch.de/themen/recht/rechtsfragen-digitales>; CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework* [Porozumienie robocze 18016 Odpowiednie do wieku ramy usług cyfrowych], dostępne pod adresem: https://www.cenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf; OECD (2021). *Children in the digital environment - Revised typology of risks* [Dzieci w środowisku cyfrowym – zmieniona typologia ryzyka]. Dostępne na stronie: https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html.

wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług.

3 STRUKTURA

16. W sekcji 4 niniejszych wytycznych określono ogólne zasady, które powinny regulować wszystkie środki wprowadzane przez dostawców platform internetowych dostępnych dla małoletnich w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich korzystających ze świadczonych przez nich usług. W sekcjach 5–8 niniejszych wytycznych określono główne środki, które zdaniem Komisji powinni wprowadzić tacy dostawcy, aby zapewnić taki wysoki poziom prywatności, bezpieczeństwa i ochrony. Należą do nich przegląd ryzyka (sekcja 5), projektowanie usług (sekcja 6), sprawozdawczość, wsparcie użytkowników i narzędzia dla opiekunów (sekcja 7) oraz zarządzanie (sekcja 8).

4 ZASADY OGÓLNE

17. Niniejsze wytyczne opierają się na następujących zasadach ogólnych, które są ze sobą wzajemnie powiązane i dostawcy platform internetowych powinni je uwzględniać całościowo we wszystkich działaniach wchodzących w zakres niniejszych wytycznych. Komisja uważa, że wszelkie środki, które dostawca platformy internetowej dostępnej dla małoletnich wprowadza w celu zapewnienia zgodności z art. 28 ust. 1 rozporządzenia (UE) 2022/2065, powinny być zgodne z następującymi zasadami ogólnymi.
 - a. **Proporcjonalność i adekwatność:** Art. 28 ust. 1 rozporządzenia (UE) 2022/2065 wymaga, aby wszelkie środki wprowadzone w celu zapewnienia zgodności z tym przepisem były odpowiednie i proporcjonalne w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich. Ponieważ różne platformy internetowe mogą być źródłem różnych rodzajów ryzyka dla małoletnich, stosowanie wszystkich lub tylko niektórych środków opisanych w niniejszych wytycznych nie zawsze będzie proporcjonalne lub odpowiednie w przypadku wszystkich dostawców platform internetowych. Ustalenie, czy dany środek jest proporcjonalny i odpowiedni, w szczególności gdy wiąże się z ingerencją w prawa podstawowe jednostki, będzie wymagało przeprowadzenia przez każdego dostawcę indywidualnego

przeglądu: (i) ryzyka dla prywatności, bezpieczeństwa i ochrony małoletnich, które stwarza jego platforma internetowa lub jej części, z uwzględnieniem m.in. wielkości, zasięgu i rodzaju świadczonej przez niego usługi oraz jej charakteru, zamierzonego lub aktualnego wykorzystania, jej szczególnych funkcji oraz bazy użytkowników danej usługi, (ii) wpływu środka na prawa dziecka oraz inne prawa i wolności zapisane w Karcie praw podstawowych Unii Europejskiej („Karta”); oraz (iii) potrzeby oparcia takich środków na najwyższych dostępnych normach i istniejących dobrych praktykach, a także uwzględnienia w nich perspektywy i praw dziecka (zob. sekcja 5 dotycząca przeglądu ryzyka).

b. Ochrona praw dziecka: Prawa te są zapisane w Karcie, która gwarantuje ochronę praw dziecka przy wdrażaniu prawa Unii, oraz w Konwencji ONZ o prawach dziecka, którą ratyfikowały wszystkie państwa członkowskie ⁽¹⁸⁾. Prawa dziecka stanowią integralną część praw człowieka, przy czym wszystkie te prawa są ze sobą wzajemnie powiązane, współzależne i niepodzielne. Zgodnie z art. 24 Karty we wszystkich działaniach dotyczących dzieci, zarówno podejmowanych przez władze publiczne, jak i instytucje prywatne, należy przede wszystkim uwzględnić najlepszy interes dziecka. W związku z tym w celu zapewnienia, aby środki służące osiągnięciu wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich na platformie internetowej były odpowiednie i proporcjonalne, należy uwzględnić wszystkie prawa dziecka, a przede wszystkim uwzględnić najlepszy interes dziecka. Zakazana jest wszelka dyskryminacja w szczególności ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną, zgodnie z art. 21 Karty. Prawa dziecka obejmują np. prawo do ochrony ⁽¹⁹⁾, niedyskryminacji, włączenia społecznego, prywatności, dostępu

⁽¹⁸⁾ W odniesieniu do środowiska cyfrowego prawa te omówił szerzej Komitet Praw Dziecka ONZ w komentarzu ogólnym nr 25. Biuro Wysokiego Komisarza Narodów Zjednoczonych ds. Praw Człowieka (2021). Komentarz ogólny nr 25 (2021) w sprawie praw dzieci w odniesieniu do środowiska cyfrowego. Dostępne na stronie: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>.

⁽¹⁹⁾ Dzieci mają prawo do takiej ochrony i opieki, jaka jest konieczna dla ich dobra (art. 24 Karty).

do informacji i edukacji, wolności wypowiedzi i uczestnictwa ⁽²⁰⁾ oraz prawo, by jego opinie uwzględniano we wszystkich sprawach, które go dotyczą ⁽²¹⁾.

c. Uwzględnianie prywatności, bezpieczeństwa i ochrony już w fazie projektowania: przy projektowaniu, rozwijaniu i świadczeniu swoich usług dostawcy platform internetowych dostępnych dla małoletnich powinni uwzględniać wysokie normy prywatności, bezpieczeństwa i ochrony ⁽²²⁾. Koncepcje uwzględniane w fazie projektowania mają na celu wykorzystanie wpływu dostawców platform internetowych, projektantów i decydentów do kształtowania rozwoju produktów i usług w sposób zapewniający priorytetowe traktowanie wartości sprzyjających dobrostanowi człowieka. Odnoszą się one do domyślnego uwzględnienia prywatności, bezpieczeństwa i ochrony w projektowaniu struktury organizacji, a także produktów i usług, ich funkcjonowaniu oraz zarządzaniu nimi od samego początku ⁽²³⁾.

d. Projektowanie dostosowane do wieku: dostawcy platform internetowych dostępnych dla małoletnich powinni projektować swoje usługi tak, aby dostosować je do rozwojowych, poznawczych i emocjonalnych potrzeb małoletnich, przy jednoczesnym zapewnieniu im bezpieczeństwa, prywatności i ochrony. Projektowanie dostosowane do wieku zapewnia rozwiązania odpowiednie dla dzieci,

⁽²⁰⁾ Mogą one swobodnie wyrażać swoje poglądy. Poglądy te są brane pod uwagę w sprawach, które ich dotyczą, stosownie do ich wieku i stopnia dojrzałości (art. 24 Karty).

⁽²¹⁾ W związku z tym Komisja przypomina o znaczeniu dostępności, w tym w zakresie uregulowanym w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i aplikacji mobilnych organów sektora publicznego („dyrektywa w sprawie dostępności stron internetowych”), a także udziału dzieci w całym procesie projektowania, wdrażania i oceny wszystkich środków na rzecz bezpieczeństwa, ochrony i prywatności dotyczących dzieci w internecie.

⁽²²⁾ Zgodnie z art. 25 RODO podmioty przetwarzające dane osobowe małoletnich muszą już wdrażać odpowiednie środki organizacyjne i techniczne w celu ochrony praw osób, których dane dotyczą (ochrona danych w fazie projektowania oraz domyślna ochrona danych). Przestrzeganie tego obowiązku jest egzekwowane przez właściwe organy ochrony danych zgodnie z art. 51 RODO. Zob. Wytyczne EROD 4/2019 w sprawie art. 25 „Uwzględnianie ochrony danych w fazie etapie projektowania oraz domyślna ochrona danych”. Dostępne na stronie: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

⁽²³⁾ OECD (2024), *Towards Digital Safety by Design for Children* [„W kierunku bezpieczeństwa cyfrowego w fazie projektowania dla dzieci”]. Dostępne na stronie: <https://doi.org/10.1787/c167b650-en>.

biorąc pod uwagę ich prawa i dobrostan, a także ich różnorodność i konkretny wiek lub etap rozwoju, jak również uwzględniając zmieniające się zdolności dzieci ⁽²⁴⁾.

5 PRZEGLĄD RYZYKA

18. Niejednorodny charakter platform internetowych i różnorodność kontekstów mogą wymagać odrębnych podejść, przy czym niektóre środki są lepiej dostosowane do niektórych platform niż inne. W przypadku gdy dostawca platformy internetowej dostępnej dla małoletnich decyduje, w jaki sposób zapewnić małoletnim na swojej platformie wysoki poziom bezpieczeństwa, prywatności i ochrony, oraz określa odpowiednie i proporcjonalne środki służące do osiągnięcia tego celu, dostawca ten, zdaniem Komisji, powinien co najmniej określić i uwzględnić:
 - a. Prawdopodobieństwo, że małoletni będą mieli dostęp do świadczonej przez niego usługi, zwłaszcza biorąc pod uwagę jej charakter, cel, zamierzone wykorzystanie, a także kryteria istotne dla ustalenia, czy usługa jest dostępna dla małoletnich.
 - b. Rzeczywisty lub potencjalny wpływ na prywatność, bezpieczeństwo i ochronę małoletnich, jaki platforma internetowa może wywierać lub powodować, w oparciu o typologię 5C dotyczącą ryzyka dla dzieci w internecie (zob. załącznik). Obejmuje to zbadanie, w jaki sposób poszczególne aspekty platformy mogą powodować takie ryzyko, jakie jest jego prawdopodobieństwo i dotkliwość, a także wzięcie pod uwagę pozytywnego wpływu tych aspektów na prawa i dobrostan dzieci, z uwzględnieniem wieku i zmieniających się zdolności dzieci. Na przykład istotne mogą być takie aspekty, jak cel platformy, jej struktura, interfejs, propozycja wartości, marketing, cechy, funkcjonalności, liczba i rodzaj użytkowników oraz zastosowania (rzeczywiste i oczekiwane).

⁽²⁴⁾ Wymaga to obrania za priorytet cech, funkcjonalności, treści lub modeli, które odpowiadają zmieniającym się zdolnościom dzieci, a także uwzględnienia różnic społeczno-kulturowych. Projektowanie dostosowane do wieku ma kluczowe znaczenie dla prywatności, bezpieczeństwa i ochrony dzieci: np. bez dostosowanych do ich wieku informacji na ten temat dzieci mogą nie być w stanie zrozumieć funkcji, ustawień lub innych narzędzi z zakresu prywatności lub bezpieczeństwa ani korzystać z nich. CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework* [Porozumienie robocze 18016 Odpowiednie do wieku ramy usług cyfrowych], dostępne na stronie: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf; informacje o wieku i etapach rozwojowych dostępne m.in. w załączniku do *Niderlandzkiego Kodeksu Dziecka*. Dostępne na stronie: <https://codevoorkinderrechten.waag.org/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf>.

Powinno to obejmować określenie poziomu ryzyka dla małoletnich na platformie (np. niskiego, średniego lub wysokiego) w oparciu o jasne kryteria, zgodnie z istniejącymi normami i najlepszymi praktykami, na przykład w odniesieniu do oceny wpływu na prawa dziecka, o której mowa w pkt 22.

- c. Środki, które dostawca już stosuje w celu zapobiegania takiemu ryzyku i zmniejszania go.
- d. Ewentualne środki dodatkowe określone w przeglądzie jako odpowiednie i proporcjonalne w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich korzystających ze świadczonej przez niego usługi. Środki, które dostawcy usług mogą być zmuszeni wprowadzić, powinny uwzględniać ryzyko dla prywatności, bezpieczeństwa i ochrony wynikające z doświadczeń małoletnich związanych z usługą, w tym ryzyko wynikające z działań innych użytkowników usługi.
- e. W jaki sposób środki są zgodne z ogólnymi zasadami określonymi w sekcji 4.
- f. Wskaźniki, które umożliwiają dostawcy monitorowanie w miarę upływu czasu skuteczności środków wprowadzonych w celu przeciwdziałania niektórym czynnikom ryzyka.
- g. Potencjalny pozytywny i negatywny wpływ na prawa dzieci lub innych użytkowników, jaki wywierają wszelkie środki stosowane przez dostawcę obecnie oraz ewentualne środki dodatkowe, przy jednoczesnym zapewnieniu, aby prawa te nie były nieproporcjonalnie lub nadmiernie ograniczane, a pozytywne skutki mogły być maksymalizowane. Prawa dzieci lub innych użytkowników, które mogą zostać naruszone przez niektóre środki, to np. prawo dzieci do uczestnictwa, prywatności, ochrony danych osobowych, wolności wypowiedzi i informacji. Jest to istotne przy określaniu proporcjonalności środków.

19. Przeprowadzając ten przegląd, dostawcy platform internetowych dostępnych dla małoletnich powinni przede wszystkim uwzględnić najlepszy interes dziecka ⁽²⁵⁾,

⁽²⁵⁾ Art. 3 Konwencji ONZ o prawach dziecka; art. 24 Karty. Prawo dziecka do tego, aby jego najlepszy interes oceniano i uwzględniano przede wszystkim przy rozważaniu różnych interesów w celu podjęcia decyzji w danej kwestii dotyczącej dziecka, grupy zidentyfikowanych lub niezidentyfikowanych dzieci

zgodnie z Kartą, oraz inne zasady Konwencji ONZ o prawach dziecka ⁽²⁶⁾, a także pozostałe odpowiednie wytyczne Unii w tym zakresie ⁽²⁷⁾. Należy dążyć do uwzględnienia perspektywy dzieci poprzez dążenie do ich zaangażowania, a także perspektywy opiekunów, przedstawicieli innych potencjalnie dotkniętych grup oraz innych odpowiednich ekspertów i zainteresowanych stron.

20. Dostawcy powinni brać pod uwagę najbardziej aktualne dostępne informacje i ustalenia pochodzące ze źródeł naukowych i akademickich, w tym poprzez wykorzystanie innych odpowiednich ocen przeprowadzonych przez dostawcę. Powinni przestrzegać zasady ostrożności, jeżeli istnieją uzasadnione przesłanki wskazujące na to, że dana praktyka, cecha lub projekt stwarzają ryzyko dla dzieci, wprowadzając środki w celu zapobiegania takiemu ryzyku lub zmniejszania go, dopóki nie pojawią się dowody na to, że skutki takiej praktyki, cechy lub projektu nie są szkodliwe dla dzieci.
21. Dostawcy powinni przeprowadzać przegląd okresowo, a co najmniej raz w roku lub za każdym razem, gdy wprowadzają istotne zmiany w projekcie platformy ⁽²⁸⁾ lub dowiadują się o innych okolicznościach, które mają wpływ na projekt i funkcjonowanie platformy, istotnych dla zapewnienia wysokiego poziomu

lub ogólnie dzieci. W razie potrzeby ustalenia dotyczące najlepszego interesu nie powinny być dokonywane przez przedsiębiorstwa, lecz opierać się na działaniach podejmowanych przez właściwe organy. LSE Digital Futures for Children (2024), *The Best interests of the child in the digital environment* [Najlepszy interes dziecka w środowisku cyfrowym]. Dostępne na stronie: <https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf>.

- ⁽²⁶⁾ Niedyskryminacja: Prawa dziecka mają zastosowanie do każdego dziecka, bez żadnej dyskryminacji, zgodnie z art. 21 Karty. Prawa dziecka, zgodnie z art. 24 Karty, obejmują prawo dzieci do takiej ochrony i opieki, jaka jest niezbędna dla ich dobra; dzieci mogą swobodnie wyrażać swoje poglądy. Poglądy te są brane pod uwagę w sprawach, które ich dotyczą, stosownie do ich wieku i stopnia dojrzałości; we wszystkich działaniach dotyczących dzieci, zarówno podejmowanych przez władze publiczne, jak i instytucje prywatne, należy przede wszystkim uwzględnić najlepszy interes dziecka. Prawa dzieci obejmują również, tak jak prawa każdego człowieka, prawo do życia zgodnie z art. 2 Karty oraz prawo do poszanowania ich integralności fizycznej i psychicznej zgodnie z art. 3 Karty. Prawa dziecka są również zapisane i doprecyzowane w Konwencji ONZ o prawach dziecka, którą ratyfikowały wszystkie państwa członkowskie.
- ⁽²⁷⁾ Komisja przypomina w szczególności wytyczne EROD dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679.
- ⁽²⁸⁾ Przykłady istotnych zmian to: wprowadzenie nowych cech wpływających na interakcję z użytkownikiem, modyfikacje systemów rekomendacji, ustawień kont, moderowania, zgłaszania lub innych cech projektu, które znacząco zmieniłyby doświadczenia dzieci na platformie, zmiany w praktykach gromadzenia danych, rozszerzenie na nowe grupy użytkowników, integracja narzędzi generatywnej sztucznej inteligencji lub zmiany związane ze środkami potwierdzania wieku lub ich dostawcami.

prywatności, bezpieczeństwa i ochrony małoletnich na ich platformie internetowej. Dostawcy usług powinni udostępniać przegląd ryzyka odpowiednim organom nadzorczym i publikować jego wyniki bez ujawniania wrażliwych danych operacyjnych lub związanych z bezpieczeństwem najpóźniej przed przeprowadzeniem kolejnego przeglądu, a także rozważyć przekazanie go do wglądu niezależnym ekspertom lub odpowiednim zainteresowanym stronom.

22. W przeprowadzaniu tego przeglądu dostawcom mogą pomóc istniejące normy i narzędzia do przeprowadzania ocen wpływu na prawa dziecka. Należą do nich np. szablony, formularze i inne wytyczne udostępniane przez UNICEF ⁽²⁹⁾, niderlandzkie Ministerstwo Spraw Wewnętrznych i Relacji w Królestwie (BZK) ⁽³⁰⁾ lub europejski organ normalizacyjny CEN-CENELEC ⁽³¹⁾. Komisja może wydawać dodatkowe wytyczne lub udostępniać instrumenty, aby wspierać dostawców w przeprowadzaniu przeglądu, w tym za pomocą specjalnych narzędzi do oceny wpływu na prawa dziecka. Do czasu publikacji niniejszych wytycznych dostawcy mogą wykorzystywać do celów tych ocen istniejące narzędzia i najlepsze praktyki.
23. W przypadku bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych przegląd ryzyka można również przeprowadzić w ramach ogólnej oceny ryzyka systemowego na podstawie art. 34 rozporządzenia (UE) 2022/2065, która uzupełni przegląd ryzyka przeprowadzany zgodnie z niniejszymi wytycznymi i wykroczy poza jego zakres.

⁽²⁹⁾ UNICEF (2024). *Children's rights impact assessment: A tool to support the design of AI and digital technology that respects children's rights* [Ocena wpływu na prawa dziecka: narzędzie wspierające projektowanie sztucznej inteligencji i technologii cyfrowej z poszanowaniem praw dziecka.]. Dostępne na stronie: <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA>; (2021) MO-CRIA: *Child Rights Impact Self-Assessment Tool for Mobile Operators* [Narzędzie samooceny wpływu na prawa dziecka dla operatorów mobilnych], dostępne na stronie: <https://www.unicef.org/reports/mo-cria-child-rights-impact-self-assessment-tool-mobile-operators>.

⁽³⁰⁾ Niderlandzkie Ministerstwo Spraw Wewnętrznych i Relacji w Królestwie (BZK) (2024). *Child Rights Impact Assessment (Fillable Form)* [Ocena wpływu na prawa dziecka (formularz do wypełnienia)]. Dostępne na stronie: <https://www.nldigitalgovernment.nl/document/childrens-rights-impact-assessment-fill-in-document/>.

⁽³¹⁾ Zob. w szczególności rozdział 14 CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework* [Porozumienie robocze 18016 Odpowiednie do wieku ramy usług cyfrowych], dostępne na stronie: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

6 PROJEKTOWANIE USŁUG

6.1 Potwierdzanie wieku

6.1.1 Wprowadzenie i terminologia

24. W ostatnich latach zachodziły szybkie zmiany technologiczne, dzięki którym dostawcy platform internetowych mogą potwierdzać wiek użytkowników bardziej lub mniej precyzyjnymi, wiarygodnymi i odpornymi sposobami. Środki te powszechnie określa się jako „potwierdzanie wieku” ⁽³²⁾.
25. Komisja uważa, że środki ograniczające dostęp ze względu na wiek są skutecznym sposobem zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich na platformach internetowych. W tym zakresie narzędzia potwierdzania wieku mogą pomóc dostawcom w egzekwowaniu ograniczeń dostępu dla użytkowników poniżej określonego wieku, aby chronić małoletnich przed dostępem do nieodpowiednich do wieku treści w internecie, takich jak hazard lub pornografia, lub przed narażeniem na inne zagrożenia, takie jak nagabywanie dla celów seksualnych.
26. Narzędzia potwierdzania wieku mogą również pomagać dostawcom w uniemożliwianiu osobom dorosłym dostępu do niektórych platform przeznaczonych dla małoletnich, z wyjątkiem sytuacji, w których odbywa się to w uzasadnionych celach rodzicielskich, edukacyjnych lub nadzorczych, zmniejszając w ten sposób ryzyko, że osoby dorosłe będą podawać się za małoletnich lub działać na szkodę małoletnich.
27. Ponadto narzędzia potwierdzania wieku mogą być wykorzystywane jako element dostosowanego do wieku projektowania samej usługi, przyczyniając się tym samym do powstania bezpieczniejszych i lepiej dostosowanych do potrzeb dzieci przestrzeni internetowych. W takich przypadkach narzędzia te można wykorzystać do zapewnienia dzieciom dostępu wyłącznie do określonych treści, cech lub czynności,

⁽³²⁾ Komisja Europejska: Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii, Content and Technology, Center for Law and Digital Technologies (eLaw), LLM, Raiz Shaffique, M. i van der Hof, S. (2024). *Mapping age assurance typologies and requirements – Research report* [Identyfikacja typologii i wymogów w zakresie potwierdzania wieku – sprawozdanie z badań naukowych]. Dostępne na stronie: <https://data.europa.eu/doi/10.2759/455338>.

które są dla nich odpowiednie, biorąc pod uwagę ich wiek i zmieniające się możliwości.

28. Należy rozróżnić, z jednej strony, ograniczenie wiekowe, ze względu na które dostęp do platformy lub jej części mają tylko użytkownicy poniżej lub powyżej określonego wieku, a z drugiej strony metody potwierdzania wieku służące do określenia wieku użytkownika.
29. Najpowszechniejsze środki potwierdzania wieku, które są obecnie dostępne i stosowane przez platformy internetowe, dzielą się na trzy szerokie kategorie: oświadczenie własne, szacowanie wieku i weryfikację wieku.
 - a. **Oświadczenie własne** to kategoria obejmująca metody, które polegają na tym, że dana osoba podaje swój wiek lub potwierdza swój przedział wiekowy – albo dobrowolnie podając datę urodzenia lub wiek, albo deklarując, że przekroczyła określony wiek, zwykle w drodze kliknięcia przycisku w internecie.
 - b. **Szacowanie wieku** obejmuje metody umożliwiające dostawcy ustalenie, że użytkownik prawdopodobnie jest w określonym wieku, mieści się w określonym przedziale wiekowym lub jest w wieku powyżej lub poniżej określonego progu⁽³³⁾.
 - c. **Weryfikacja wieku** to system oparty na identyfikatorach fizycznych lub zweryfikowanych źródłach identyfikacji, które zapewniają wysoki stopień pewności przy określaniu wieku użytkownika.
30. Środki szacowania wieku i weryfikacji wieku różnią się od siebie przede wszystkim poziomem dokładności. Weryfikacja wieku daje pewność co do wieku użytkownika, natomiast szacowanie wieku zapewnia przybliżenie wieku użytkownika. Dokładność technologii szacowania wieku może być różna i poprawiać się w miarę postępu technologicznego.

⁽³³⁾ tamże; CEN-CENELEC (2023). *Workshop Agreement 18016 Age Appropriate Digital Services Framework* [Porozumienie robocze 18016 Odpowiednie do wieku ramy usług cyfrowych]: https://www.cenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

6.1.2 Ustalenie, czy należy wprowadzić ograniczenia dostępu wsparte środkami potwierdzania wieku

31. Przed podjęciem decyzji, czy wprowadzić jakiegokolwiek ograniczenia dostępu ze względu na wiek, w oparciu o metody potwierdzania wieku, dostawcy platform internetowych dostępnych dla małoletnich powinni zawsze przeprowadzić ocenę w celu ustalenia, czy taki środek jest odpowiedni do zapewnienia małoletnim wysokiego poziomu prywatności, bezpieczeństwa i ochrony w ramach świadczonej przez nich usługi oraz czy jest on proporcjonalny lub czy taki wysoki poziom można już osiągnąć poprzez zastosowanie innych, nie tak daleko idących środków ⁽³⁴⁾. W związku z tym Komisja jest zdania, że dostawcy powinni rozważyć ograniczenia dostępu ze względu na wiek wsparte środkami potwierdzania wieku jako narzędzie uzupełniające środki określone w innych sekcjach niniejszych wytycznych. Innymi słowy, same ograniczenia dostępu i potwierdzanie wieku nie mogą zastąpić środków zalecanych gdzie indziej w niniejszych wytycznych.
32. Taka ocena powinna zapewniać, aby wszelkie ograniczenia w korzystaniu z podstawowych praw i wolności przez odbiorców, w szczególności małoletnich, były proporcjonalne. W związku z tym Komisja uważa, że dostawcy platform internetowych powinni podawać wyniki takiej oceny do wiadomości publicznej w interfejsie internetowym świadczonej przez siebie usługi, zarówno w przypadku gdy z oceny wynika, że nie jest wymagane ograniczenie dostępu wsparte potwierdzaniem wieku, jak i w przypadku gdy takie ograniczenie byłoby odpowiednim i proporcjonalnym środkiem.
33. Komisja zauważa, że mniejsza dokładność rozwiązań w zakresie szacowania wieku nie oznacza automatycznie mniejszego wpływu na podstawowe prawa i wolności odbiorców, ponieważ mniej dokładne rozwiązania mogą wiązać się z przetwarzaniem większej ilości danych osobowych niż rozwiązania dokładniejsze. Mogą one również uniemożliwiać niektórym dzieciom dostęp do platform internetowych, do których w przeciwnym razie mogłyby mieć dostęp ze względu na niższy poziom dokładności. W związku z tym biorąc pod uwagę metody szacowania wieku, które wymagają przetwarzania danych osobowych, dostawcy platform internetowych dostępnych dla małoletnich powinni zapewnić, aby należycie wdrażano zasady ochrony danych

⁽³⁴⁾ W przeprowadzeniu tej oceny dostawcom platform internetowych może pomóc przegląd ryzyka i narzędzia oceny wpływu na prawa dziecka przedstawione w sekcji 5 dotyczącej przeglądu ryzyka.

zachowujące skuteczność z upływem czasu, w szczególności dotyczące minimalizacji danych, a ponadto powinni uwzględnić oświadczenie Europejskiej Rady Ochrony Danych (EROD) w sprawie potwierdzania wieku ⁽³⁵⁾.

34. Komisja jest zdania, że w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich korzystających ze świadczonych przez nich usług dostawcy platform internetowych dostępnych dla małoletnich, którzy uznają ograniczenia dostępu oparte na metodach potwierdzania wieku za konieczne i proporcjonalne, powinni udostępniać informacje na temat wszelkich wybranych przez siebie rozwiązań w zakresie potwierdzania wieku oraz ich adekwatności i skuteczności. Powinni również udostępniać przegląd wskaźników efektywności stosowanych do pomiaru ich adekwatności i skuteczności, takich jak odsetek wyników fałszywie dodatnich i fałszywie ujemnych oraz wskaźniki dokładności i czułości.
35. Należy przewidzieć udział dzieci w opracowywaniu, wdrażaniu i ocenie ograniczeń wiekowych oraz metod potwierdzania wieku.
36. W przypadku platform internetowych dostępnych dla małoletnich istnieje możliwość, że tylko niektóre z udostępnianych przez nie treści, sekcji lub funkcji stanowią zagrożenie dla małoletnich, ewentualnie w pewnych częściach platformy ryzyko może być zmniejszane innymi środkami, podczas gdy w innych częściach nie jest to możliwe. W takich sytuacjach, zamiast ograniczania wieku w odniesieniu do usługi jako całości, dostawcy takich platform internetowych powinni ocenić, które treści, sekcje lub funkcje na ich platformach stwarzają ryzyko dla małoletnich i wdrożyć ograniczenia dostępu wsparte metodami potwierdzania wieku, aby zmniejszyć takie ryzyko dla małoletnich w sposób proporcjonalny i odpowiedni. Na przykład części usług mediów społecznościowych obejmujące treści, sekcje lub funkcje, które mogą stwarzać ryzyko dla małoletnich, takie jak sekcje mediów społecznościowych przeznaczone tylko dla dorosłych, sekcje zawierające informacje handlowe przeznaczone tylko dla dorosłych lub lokowanie przez influencerów produktu

⁽³⁵⁾ Zob. oświadczenie EROD nr 1/2025 w sprawie potwierdzania wieku. Dostępne na stronie: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_pl

przeznaczonego tylko dla dorosłych, powinny być udostępniane wyłącznie dorosłym użytkownikom, których wiek należycie zweryfikowano.

6.1.3 Ustalanie odpowiednich metod potwierdzania wieku

6.1.3.1 Weryfikacja wieku

37. W następujących okolicznościach, biorąc pod uwagę fakt, że ochrona małoletnich stanowi ważny cel polityki Unii, któremu wyraz daje rozporządzenie (UE) 2022/2065, co znajduje odzwierciedlenie w motywie 71, stosowanie ograniczeń dostępu wspartych metodami **weryfikacji wieku** stanowi, zdaniem Komisji, odpowiedni i proporcjonalny środek zapewniający wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich:
- a. W sytuacji, gdy niektóre produkty lub usługi stwarzają wysokie ryzyko dla małoletnich i ryzyka tego nie można zmniejszyć za pomocą mniej restrykcyjnych środków, z uwzględnieniem mających zastosowanie przepisów unijnych i krajowych, np. w przypadku:
 - i. sprzedaży alkoholu, wyrobów tytoniowych lub wyrobów zawierających nikotynę, narkotyków,
 - ii. dostępu do wszelkiego rodzaju treści pornograficznych,
 - iii. dostępu do gier hazardowych.
 - b. W przypadku gdy ze względu na zidentyfikowane ryzyko dla małoletnich warunki korzystania z usług lub inne zobowiązania umowne dotyczące usługi wymagają, aby użytkownik uzyskujący dostęp do usługi miał co najmniej 18 lat, nawet jeżeli nie obowiązuje ustanowiony przez prawo formalny próg wiekowy.
 - c. We wszelkich innych okolicznościach, w których dostawca platformy internetowej dostępnej dla małoletnich zidentyfikował ryzyko dla prywatności, bezpieczeństwa lub ochrony małoletnich, w tym ryzyko dotyczące treści, zachowania i ryzyko dla konsumentów, a także ryzyko związane z kontaktem (np. odnoszące się do takich funkcji jak czat na żywo, udostępnianie obrazów/materiałów wideo, anonimowe wiadomości), w przypadku gdy za pomocą innych mniej inwazyjnych środków ryzyka tego nie można zmniejszyć

tak skutecznie, jak za pomocą ograniczeń dostępu wspartych weryfikacją wieku⁽³⁶⁾.

- d. W przypadku gdy prawo Unii lub prawo krajowe, zgodnie z prawem Unii, określa minimalny wiek dostępu do niektórych produktów lub usług oferowanych lub wyświetlanych w jakikolwiek sposób na platformie internetowej, w tym wyraźnie określonych kategorii internetowych mediów społecznościowych⁽³⁷⁾.

38. Uzupełnieniem technologii weryfikacji wieku mogą być metody szacowania wieku – można je stosować równolegle lub jako tymczasowe rozwiązanie alternatywne, w szczególności w przypadkach, gdy nie są jeszcze łatwo dostępne środki weryfikacji zgodne z kryteriami skuteczności rozwiązań w zakresie potwierdzania wieku przedstawionymi w sekcji 6.1.4, ze szczególnym naciskiem na ochronę prawa użytkowników do prywatności i ochrony danych, a także na dokładność. Ten okres przejściowy nie powinien wykraczać poza pierwszy przegląd niniejszych wytycznych⁽³⁸⁾. Np. platformy oferujące treści przeznaczone dla dorosłych mogą stosować metody szacowania wieku *ex ante*, jeżeli są w stanie wykazać, że metody te są porównywalne z metodami weryfikacji wieku, w odniesieniu do kryteriów określonych w sekcji 6.1.4, przy braku skutecznych środków weryfikacji wieku⁽³⁹⁾. Komisja może w odpowiednim czasie uzupełnić niniejsze wytyczne o analizę

⁽³⁶⁾ Zagrożenia te można zidentyfikować w drodze przeglądu ryzyka określonego w sekcji 5.

⁽³⁷⁾ W tym kontekście Komisja przypomina o obowiązkach nałożonych na państwa członkowskie na mocy dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1) oraz o odpowiednich procedurach dotyczących projektów przepisów technicznych ustanowionych we tej dyrektywie.

⁽³⁸⁾ Komisja testuje obecnie unijne rozwiązanie służące do weryfikacji wieku, aby ułatwić weryfikację wieku zgodnie ze standardem wymaganym w niniejszych wytycznych przed udostępnieniem europejskiego portfela tożsamości cyfrowej. Inne rozwiązania, zgodne ze standardem określonym w niniejszych wytycznych, mogą być dostępne na rynku lub w poszczególnych państwach członkowskich, ale nie w innych. Dostawcy platform internetowych, którzy udowodnią wystąpienie tej okoliczności, powinni i tak zacząć testować i stosować metody weryfikacji wieku, które spełniają kryteria określone w sekcji 6.1.4, gdy tylko metody takie staną się dostępne. Ten okres przejściowy można dostosować w związku z wprowadzeniem unijnego rozwiązania służącego do weryfikacji wieku.

⁽³⁹⁾ . Przegląd różnych metod szacowania wieku jest dostępny w dokumencie Komisji Europejskiej: Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii, Content and Technology, Center for Law and Digital Technologies (eLaw), LLM, Raiz Shaffique, M. i van der Hof, S. (2024) *Mapping age assurance typologies and requirements – Research report* [Identyfikacja typologii i wymogów w zakresie potwierdzania wieku – sprawozdanie z badań naukowych]. Dostępne na stronie: <https://data.europa.eu/doi/10.2759/455338>.

techniczną głównych istniejących metod szacowania wieku, które są obecnie dostępne, w świetle kryteriów przedstawionych w sekcji 6.1.4.

6.1.3.2 Technologie weryfikacji wieku

39. Weryfikację wieku należy traktować jako odrębny, oddzielny proces, który nie jest powiązany z innymi działaniami w zakresie gromadzenia danych prowadzonymi przez platformy internetowe. Weryfikacja wieku nie powinna uprawniać dostawców platform internetowych do przechowywania danych osobowych wykraczających poza informacje o grupie wiekowej użytkownika.
40. Jak wyjaśniono bardziej szczegółowo w sekcji 6.1.4, każda metoda potwierdzania wieku powinna być odporna, a zatem niełatwa do obejścia, aby można ją było uznać za odpowiednią i proporcjonalną. Metoda, która jest łatwa do obejścia przez małoletnich, nie będzie uznawana za skuteczny środek potwierdzania wieku.
41. Metody oparte na zweryfikowanych i zaufanych identyfikatorach wydawanych przez rząd, bez przekazywania platformie dodatkowych danych osobowych, mogą stanowić skuteczną metodę weryfikacji wieku, o ile opierają się na zanonimizowanych tokenach wieku ⁽⁴⁰⁾. Takie tokeny powinny być wydawane po wiarygodnej weryfikacji wieku danej osoby, przy czym wydawać je powinna niezależna osoba trzecia, a nie dostawca platformy internetowej, zwłaszcza gdy oferuje ona dostęp do treści dla dorosłych. Komisja uważa, że protokoły kryptograficzne, takie jak rotacja kluczy lub dowody z wiedzą zerową ⁽⁴¹⁾, stanowią odpowiednią podstawę dla potwierdzania wieku bez przekazywania danych osobowych.

⁽⁴⁰⁾ Usługodawca musi jedynie wiedzieć, czy użytkownik przekroczył próg wiekowy, czy nie. Rozwiązanie to należy wdrożyć za pomocą podejścia obejmującego tokeny, opartego na udziale dostawcy będącego osobą trzecią, przy czym usługodawca widzi jedynie funkcjonalny wynik procesu potwierdzania wieku (np. „powyżej” lub „poniżej” progu wiekowego). Dostawca usług będący osobą trzecią przeprowadza kontrolę wieku i przekazuje użytkownikowi „token wieku”, który użytkownik może przedstawić usługodawcy bez konieczności ponownego udowadniania swojego wieku. Token wieku może zawierać różne cechy użytkownika i informacje o tym, kiedy, gdzie lub w jaki sposób przeprowadzono kontrolę wieku. Zob. również oświadczenie EROD 1/2025 w sprawie potwierdzania wieku. Dostępne na stronie: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_pl

⁽⁴¹⁾ Dowód z wiedzą zerową to procedura, w której jedna ze stron (dowodzący) może wykazać drugiej stronie (weryfikującemu) prawdziwość danego stwierdzenia bez ujawniania innych informacji poza potwierdzeniem, że to stwierdzenie jest prawdziwe.

42. Państwa członkowskie są obecnie w trakcie zapewniania europejskiego portfela tożsamości cyfrowej ⁽⁴²⁾ dla każdego swojego obywatela, mieszkańca i przedsiębiorstwa. Przyszłe europejskie portfele tożsamości cyfrowej będą stanowić bezpieczny, niezawodny i prywatny środek identyfikacji elektronicznej w Unii. Po ich wprowadzeniu można będzie ich używać do udostępnienia usług wyłącznie określonych informacji, np. że dana osoba przekroczyła określony wiek.

Europejski portfel tożsamości cyfrowej

Po wdrożeniu europejskie portfele tożsamości cyfrowej będą bezpiecznym, niezawodnym i prywatnym środkiem identyfikacji elektronicznej dla wszystkich w Unii. Każde państwo członkowskie jest zobowiązane do udostępnienia do końca 2026 r. co najmniej jednego portfela każdemu swojemu obywatelowi, mieszkańcowi i przedsiębiorstwu, co powinno pozwolić im na udowodnienie ich tożsamości oraz bezpieczne przechowywanie, udostępnianie i podpisywanie ważnych dokumentów elektronicznych. Wszystkie europejskie portfele tożsamości cyfrowej mogą przyjmować tokeny dotyczące wieku, a państwa członkowskie mogą wdrażać usługi wydawania takich tokenów.

43. Aby ułatwić weryfikację wieku przed udostępnieniem europejskich portfeli tożsamości cyfrowej, Komisja testuje obecnie unijne rozwiązanie służące do weryfikacji wieku jako samodzielny środek weryfikacji wieku, który spełnia kryteria skuteczności rozwiązań służących do potwierdzania wieku określonych w sekcji 6.1.4. Po sfinalizowaniu unijne rozwiązanie służące do weryfikacji wieku będzie stanowić przykład zgodności i normę referencyjną dla metody weryfikacji wieku opartej na urządzeniach. Dostawców platform internetowych, co do których oczekuje się, że będą korzystać z rozwiązań służących do weryfikacji wieku w odniesieniu do świadczonych przez siebie usług, zachęca się zatem do udziału w dostępnych testach wczesnych wersji unijnego rozwiązania służącego do weryfikacji wieku – w ten sposób dostawcy ci mogą uzyskać informacje o najlepszych sposobach zapewnienia zgodności z art. 28 rozporządzenia (UE) 2022/2065.
44. Wdrażanie normy referencyjnej ⁽⁴³⁾ ustanowionej poprzez wprowadzenie unijnego rozwiązania służącego do weryfikacji wieku może odbywać się za pośrednictwem aplikacji publikowanych przez podmioty publiczne lub prywatne lub zintegrowanych z przyszłymi europejskimi portfelami tożsamości cyfrowej. Dzięki wdrożeniu tej

⁽⁴²⁾ Jak przewidziano w rozdziale II sekcja 1 rozporządzenia (UE) nr 910/2014 zmienionego rozporządzeniem (UE) 2024/1183.

⁽⁴³⁾ Norma referencyjna UE jest dostępna pod adresem <https://ageverification.dev>.

normy zostanie udostępniona technologia weryfikacji wieku, która chroni prywatność, minimalizuje dane, nie jest identyfikowalna oraz jest interoperacyjna, zgodnie z kryteriami skuteczności rozwiązań w zakresie potwierdzania wieku określonymi w sekcji 6.1.4.

Unijne rozwiązanie służące do weryfikacji wieku

Unijne rozwiązanie służące do weryfikacji wieku, obejmujące aplikację, będzie łatwą w użyciu metodą weryfikacji wieku, której można będzie używać w celu udowodnienia, że użytkownik ma 18 lat lub więcej (ponad 18 lat). Rozwiązanie to wypełni lukę istniejącą do czasu udostępnienia europejskiego portfela tożsamości cyfrowej. To solidne rozwiązanie, które chroni prywatność i jest zgodne z zasadą minimalizacji danych, będzie miało na celu ustanowienie normy w zakresie prywatności i przyjazności dla użytkownika.

Unijne rozwiązanie służące do weryfikacji wieku zapewnia punkt odniesienia pod względem zgodności w odniesieniu do dokładności rozwiązania w zakresie potwierdzania wieku, przy jednoczesnym zminimalizowaniu wpływu na prawa i wolności odbiorców.

Użytkownicy będą mogli z łatwością aktywować aplikację i uzyskać dowód na kilka różnych sposobów. Dowód potwierdza jedynie, że użytkownik ma 18 lat lub więcej. Nie wskazuje dokładnego wieku ani nie zawiera żadnych innych informacji o użytkowniku. Użytkownik może przedstawić na platformie internetowej dowód ukończenia 18. roku życia w sposób chroniący jego prywatność bez przepływu danych do dostawcy dowodu. Ponadto wprowadzone zostaną mechanizmy zapobiegające śledzeniu na platformach internetowych. Korzystanie z aplikacji jest proste. Domagając się dostępu do treści internetowych dla dorosłych użytkownik za pośrednictwem aplikacji przedstawia platformie internetowej dowód ukończenia 18. roku życia. Po zweryfikowaniu ważności dowodu platforma internetowa udziela użytkownikowi dostępu. W trakcie całego procesu tożsamość i działania użytkownika są chronione przed ujawnieniem. Dostawca zaufanych dowodów nie jest informowany o tym, do których usług internetowych użytkownik stara się uzyskać dostęp za pomocą dowodu ukończenia 18. roku życia. Podobnie dostawcy usług internetowych dla osób, które ukończyły 18. rok życia, nie są informowani o tożsamości użytkownika starającego się uzyskać dostęp, a jedynie otrzymują dowód, że użytkownik ma 18 lat lub więcej.

Unijne rozwiązanie służące do weryfikacji wieku będzie mieć również techniczną możliwość przekazywania informacji o innych cechach, np. wyników testów żywotności. W krajach, w których stosuje się ważne metody poświadczania wieku poniżej 18 lat, unijne rozwiązanie służące do weryfikacji wieku może również umożliwiać weryfikację wieku poniżej 18. roku życia.

45. Dostawcy platform internetowych dostępnych dla małoletnich mogą stosować inne metody weryfikacji wieku w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich, pod warunkiem że są one zgodne z normą referencyjną UE (opisaną w pkt 43 i 44 powyżej) i spełniają kryteria określone w sekcji 6.1.4. Unijne rozwiązanie służące do weryfikacji wieku jest przykładem metody spełniającej te kryteria.

46. Aby zapewnić zgodność z zasadami minimalizacji danych, celowości i zaufania użytkowników, dostawców platform internetowych zachęca się do przyjęcia rozwiązań umożliwiających weryfikację wieku metodą *podwójnie ślepą*. Metoda podwójnie ślepa gwarantuje, że (i) platforma internetowa nie otrzymuje dodatkowych środków identyfikacji użytkownika, a zamiast tego otrzymuje jedynie informacje umożliwiające jej potwierdzenie, czy użytkownik osiągnął wymagany próg wiekowy, oraz że (ii) dostawca rozwiązania służącego do weryfikacji wieku nie uzyskuje wiedzy na temat usług, w odniesieniu do których stosuje się dowód wieku. Takie metody mogą opierać się na lokalnym przetwarzaniu na urządzeniu, zanonimizowanych tokenach kryptograficznych lub dowodach z wiedzą zerową ⁽⁴⁴⁾.

6.1.3.3 Szacowanie wieku

47. Komisja uważa, że stosowanie metod szacowania wieku, jeżeli są one zapewniane przez niezależną stronę trzecią lub za pośrednictwem systemów poddanych odpowiedniej i niezależnej kontroli, zwłaszcza w zakresie zgodności z wymogami bezpieczeństwa i ochrony danych, a także gdy odbywa się *ex ante*, jeżeli jest to konieczne dla zagwarantowania skuteczności środka, jest odpowiednim i proporcjonalnym środkiem zapewniającym wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w następujących okolicznościach:
- a. W przypadku gdy ze względu na zidentyfikowane ryzyko dla prywatności, bezpieczeństwa i ochrony małoletnich warunki korzystania z usług platformy internetowej lub podobne zobowiązania umowne dotyczące usługi wymagają, aby wiek użytkownika uzyskującego dostęp do usługi był wyższy od

⁽⁴⁴⁾ Metody te w dużej mierze stanowią odpowiedź na apel EROD, zawarty w pkt 34 jej oświadczenia 1/2025 w sprawie potwierdzania wieku, o wprowadzenie rozwiązań zapobiegających tworzeniu powiązań i profilowaniu. Te podejścia chroniące prywatność są również preferowane przez badaczy jako skalowalne, włączające i skuteczne w minimalizowaniu ryzyka dla małoletnich przy jednoczesnym poszanowaniu praw podstawowych. Dostępne na stronie: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_pl

wymaganego wieku minimalnego, wynoszącego mniej niż 18 lat, w oparciu o dokonaną przez dostawcę ocenę ryzyka dla małoletnich na platformie ⁽⁴⁵⁾ ⁽⁴⁶⁾.

- b. W przypadku gdy dostawca platformy internetowej stwierdził na swojej platformie średni poziom ryzyka dla małoletnich, ustalony w przeglądzie ryzyka (zob. sekcja 5 dotycząca przeglądu ryzyka) ⁽⁴⁷⁾, a ryzyka tego nie można zmniejszyć za pomocą mniej restrykcyjnych środków. Komisja uważa, że będzie to miało miejsce w przypadku gdy ryzyko nie jest na tyle wysokie, aby wymagać ograniczenia dostępu w oparciu o weryfikację wieku, ale nie jest na tyle niskie, że właściwy byłby brak jakichkolwiek ograniczeń dostępu lub zastosowanie ograniczenia dostępu, które nie opiera się na żadnej metodzie potwierdzania wieku lub opiera się wyłącznie na oświadczeniu własnym. Jak wyjaśniono poniżej, oświadczenie własne nie jest uznawane za odpowiedni środek potwierdzania wieku.

Dobre praktyki

MegaBetting ⁽⁴⁸⁾ to platforma internetowa, która umożliwia użytkownikom zawieranie zakładów dotyczących wyników rzeczywistych wydarzeń. Dostawca ogranicza dostęp do świadczonej przez siebie usługi do użytkowników w wieku powyżej 18 lat, zgodnie z prawem krajowym. W celu zapewnienia, aby platforma nie była dostępna dla małoletnich, wykorzystuje się na niej unijne rozwiązanie służące do weryfikacji wieku, w ramach którego dostawca informowany jest jedynie o tym, czy użytkownik ma co najmniej 18 lat. Informacje te są generowane przez zaufanego wystawcę na podstawie krajowej identyfikacji elektronicznej użytkownika i otrzymywane z aplikacji w telefonie użytkownika. Dostawca uważa zatem, że system spełnia kryteria wysokiej skuteczności przy jednoczesnym zachowaniu prywatności użytkownika.

Złe praktyki

⁽⁴⁵⁾ Jeżeli w takich przypadkach stosuje się weryfikację wieku, pozostaje to bez uszczerbku dla wszelkich odrębnych obowiązków usługodawcy, np. wymogu oceny, czy małoletni jako konsument osiągnął wystarczający wiek, aby legalnie zawrzeć umowę. Zależy to od prawa właściwego państwa członkowskiego, w którym zamieszkuje małoletni.

⁽⁴⁶⁾ W niektórych przypadkach dostawca może mieć możliwość weryfikacji, czy małoletni został zarejestrowany przez swoich opiekunów.

⁽⁴⁷⁾ Zagrożenia te można zidentyfikować w drodze przeglądu ryzyka określonego w sekcji 5.

⁽⁴⁸⁾ Wszystkie przykłady dobrych i złych praktyk w niniejszych wytycznych odnoszą się do fikcyjnych platform internetowych.

SadMedia to internetowa platforma społecznościowa. Dostawca SadMedia postanowił zakazać dostępu do świadczonej przez siebie usługi małoletnim w wieku poniżej 13 lat. Decyzja ta wynika ze stwierdzenia średniego poziomu ryzyka, jakie platforma może stwarzać dla prywatności, bezpieczeństwa i ochrony małoletnich. Ograniczenie to zapisano w warunkach korzystania z usług SadMedia. Aby egzekwować to ograniczenie, dostawca SadMedia stosuje opracowany przez siebie model szacowania wieku, który, według niego, potrafi przewidzieć wiek użytkownika z marginesem błędu wynoszącym ± 2 lata. Ze względu na ten margines błędu dostęp do usługi uzyskuje wielu małoletnich poniżej wskazanego wieku, a jednocześnie nie uzyskuje go wielu małoletnich, którzy osiągnęli wymagany wiek. Środek potwierdzania wieku stosowany przez SadMedia nie jest wysoce skuteczny i w związku z tym nie zapewnia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich korzystających z usług SadMedia.

48. W przypadku gdy dostawca platformy internetowej dostępnej dla małoletnich ustalił, że dla osiągnięcia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich korzystających ze świadczonej przez niego usługi niezbędne są ograniczenia dostępu poparte potwierdzaniem wieku, powinien on, zdaniem Komisji, oferować na platformie więcej niż jedną metodę potwierdzania wieku, aby zapewnić użytkownikowi wybór, pod warunkiem że każda taka metoda spełnia kryteria określone w sekcji 6.1.4. Pomoże to uniknąć wykluczenia użytkowników, którzy, mimo spełnienia warunków dostępu do platformy internetowej, nie mogą korzystać z określonej metody potwierdzania wieku. Aby zwiększyć skuteczność i przyjazność dla użytkownika, oprócz innych środków ochronnych, o których mowa w niniejszych wytycznych, należy stosować odpowiednią metodę potwierdzania wieku, w miarę możliwości na etapie tworzenia konta, przy czym informacje o wieku powinny następnie służyć do zapewnienia odpowiedniego do wieku doświadczenia na platformie. Ponadto dostawcy platform internetowych powinni zapewnić użytkownikom mechanizm odwoławczy, aby mogli oni składać skargi w przypadku ewentualnych nieprawidłowych ocen wieku dokonanych przez dostawcę ⁽⁴⁹⁾.

Złe praktyki

SadMedia wykorzystuje rozwiązanie z zakresu szacowania wieku jako jeden z szeregu środków, które mają przyczynić się do wysokiego poziomu prywatności, bezpieczeństwa i ochrony. Jeżeli system szacowania wieku daje wynik negatywny, co oznacza, że użytkownik jest zbyt młody, aby skorzystać z usługi, użytkownikowi wyświetlane jest okno dialogowe zawierające wskazówkę: „Nie zgadzasz się z wynikiem? Spróbuj ponownie!” Użytkownik może wówczas ponownie poddać się testowi służącemu oszacowaniu wieku za pomocą tej samej metody. W tym przykładzie środek potwierdzania wieku nie zostałby uznany za odpowiedni ani proporcjonalny, ponieważ odbiorca nie

⁽⁴⁹⁾ Dostawca może zdecydować się na włączenie tego mechanizmu do swojego wewnętrznego systemu rozpatrywania skarg, o którym mowa w art. 20. Zob. również sekcja 7.1 niniejszego dokumentu.

ma możliwości zastosowania innej metody potwierdzania wieku ani zakwestionowania błędnej oceny.

6.1.4 Ocena adekwatności i proporcjonalności każdej metody potwierdzania wieku

49. Przed rozważeniem wprowadzenia konkretnej metody weryfikacji lub szacowania wieku do celów ograniczenia dostępu dostawcy platform internetowych dostępnych dla małoletnich powinni wziąć pod uwagę następujące cechy tej metody:

a. **Dokładność.** Jak dokładnie dana metoda określa wiek użytkownika.

Dokładność metody weryfikacji lub szacowania wieku należy oceniać na podstawie odpowiednich, jasnych i publicznie dostępnych wskaźników. Wskaźniki te są niezbędne do oceny zakresu, w jakim metoda może prawidłowo określić, czy użytkownik jest powyżej, czy poniżej określonego wieku lub do jakiego przedziału wiekowego należy dana osoba ⁽⁵⁰⁾. Dostawcy platform internetowych powinni okresowo sprawdzać, czy dokładność techniczna stosowanej metody nadal odpowiada aktualnemu stanowi rozwoju technologii.

b. **Wiarygodność.** Jak wiarygodna dana metoda jest w praktyce, w warunkach rzeczywistych.

Aby metoda była wiarygodna, powinna być dostępna stale, w każdym momencie, i działać w różnych warunkach rzeczywistych, nie tylko w idealnych warunkach testowych. Przed zastosowaniem konkretnego rozwiązania w zakresie potwierdzania wieku dostawcy platform internetowych dostępnych dla małoletnich powinni ocenić, czy wszelkie dane wykorzystywane w procesie potwierdzania wieku pochodzą z wiarygodnego źródła. Na przykład za wiarygodne nie uznano by poświadczenia wieku podpisanego przez samego użytkownika.

c. **Odporność.** Jak łatwo jest obejść daną metodę.

⁽⁵⁰⁾ Niedokładne potwierdzenie wieku może prowadzić do wykluczenia odbiorców, którzy spełniają warunki korzystania z usługi lub umożliwiać dostęp do niej odbiorcom niespełniającym warunków, pomimo wprowadzonego środka potwierdzania wieku.

Metoda, która jest *łatwa* do obejścia przez małoletnich, nie zostanie uznana za wystarczająco odporną i w związku z tym nie będzie uważana za skuteczną. Dostawcy platform internetowych dostępnych dla małoletnich powinni oceniać taki poziom „łatwości” indywidualnie dla każdego przypadku, z uwzględnieniem wieku małoletnich, do których donoszą się określone środki. Dostawcy platform internetowych dostępnych dla małoletnich powinni również oceniać, czy metoda potwierdzania wieku zapewnia bezpieczeństwo i ochronę, zgodnie z aktualnym stanem wiedzy technicznej, w celu zapewnienia integralności przetwarzanych danych dotyczących wieku.

- d. **Nieinwazyjność.** Jak inwazyjna jest dana metoda w odniesieniu do praw użytkowników.

Dostawcy platform internetowych dostępnych dla małoletnich powinni okresowo oceniać wpływ wybranej metody na prawa i wolności odbiorców, w tym ich prawo do prywatności, ochrony danych i wolności wypowiedzi ⁽⁵¹⁾. Według Europejskiej Rady Ochrony Danych i zgodnie z art. 28 ust. 3 rozporządzenia (UE) 2022/2065 ⁽⁵²⁾ dostawca powinien przetwarzać wyłącznie dane dotyczące wieku, które są absolutnie niezbędne do konkretnego celu, a potwierdzanie wieku nie powinno służyć dostawcom jako dodatkowy środek identyfikacji, lokalizacji, profilowania lub śledzenia osób fizycznych ⁽⁵³⁾. Jeżeli metoda jest bardziej inwazyjna niż inna metoda zapewniająca ten sam poziom pewności i skuteczności, należy wybrać metodę mniej inwazyjną. Obejmuje to ocenę, czy metoda zapewnia pełną przejrzystość procesu zgodnie z art. 12 rozporządzenia (UE) 2016/679 lub czy dostarcza informacje na temat użytkownika narażonego na ryzyko. W żadnym wypadku dane przetwarzane do celów ustalenia, czy użytkownik jest powyżej, czy poniżej określonego wieku, nie mogą być przechowywane ani wykorzystywane do innych celów.

⁽⁵¹⁾ Potwierdzanie wieku w sposób niewłaściwy może stwarzać nadmierne ryzyko w odniesieniu do praw odbiorców do ochrony danych i prywatności, natomiast ogólne potwierdzanie wieku mogłoby ograniczyć dostęp do usług ponad to, co jest faktycznie konieczne.

⁽⁵²⁾ Zob. motyw 71 rozporządzenia (UE) 2022/2065, w którym podkreślono potrzebę przestrzegania przez dostawców zasady minimalizacji danych przewidzianej w art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679.

⁽⁵³⁾ Zob. oświadczenie EROD 1/2025 w sprawie potwierdzania wieku, pkt 2.3 i 2.4. Dostępne na stronie: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_pl

- e. **Niedyskryminacja.** W jaki sposób dana metoda może dyskryminować niektórych użytkowników.

Dostawcy platform internetowych dostępnych dla małoletnich powinni dopilnować, aby wybrana metoda była odpowiednia i dostępna dla wszystkich małoletnich, niezależnie od niepełnosprawności, języka, pochodzenia etnicznego, płci, religii i przynależności do mniejszości.

50. Jeżeli środki potwierdzania wieku nie spełniają kryteriów określonych powyżej, nie można ich uznać za odpowiednie i proporcjonalne.
51. Rozwiązań potwierdzania wieku, które można łatwo obejść, nie należy uznawać za zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich. Ocenę taką należy przeprowadzić w zależności od wpływu, jaki platforma może mieć na prywatność, bezpieczeństwo i ochronę małoletnich. Przechowywanie poświadczenia wieku powinno również być uzależnione od ryzyka związanego z danymi platformami. Na przykład platformy internetowe przeznaczone dla osób dorosłych nie powinny umożliwiać udostępniania danych logowania do kont użytkowników, a zatem powinny potwierdzać wiek w każdym przypadku uzyskiwania dostępu do usługi.
52. Komisja uważa, że **oświadczenie własne** ⁽⁵⁴⁾ nie spełnia wszystkich powyższych wymogów, w szczególności wymogów odporności i dokładności. W związku z tym nie uważa oświadczenia własnego za odpowiednią metodę potwierdzania wieku w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich zgodnie z art. 28 ust. 1 rozporządzenia (UE) 2022/2065.
53. Ponadto Komisja uważa, że informację o wykorzystaniu strony trzeciej do potwierdzania wieku należy udostępniać małoletnim – tak jak w każdym przypadku – w sposób przystępny, widoczny i z zastosowaniem sformułowań zrozumiałych dla dziecka (zob. sekcja 8.4 dotycząca przejrzystości). Ponadto obowiązkiem dostawcy pozostaje zapewnienie skuteczności metody stosowanej przez stronę trzecią, zgodnie z powyższymi uwagami. Obejmuje to na przykład sytuacje, w których dostawca

⁽⁵⁴⁾ Komisja Europejska: Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii, Content and Technology, Center for Law and Digital Technologies (eLaw), LLM, Raiz Shaffique, M. i van der Hof, S. (2024) *Mapping age assurance typologies and requirements – Research report* [Identyfikacja typologii i wymogów w zakresie potwierdzania wieku – sprawozdanie z badań naukowych]. Dostępne na stronie: <https://data.europa.eu/doi/10.2759/455338>.

zamierza wykorzystywać rozwiązania zapewniane przez systemy operacyjne lub operatorów urządzeń.

6.2 Rejestracja

54. Rejestracja lub uwierzytelnianie mogą mieć wpływ na to, czy i w jaki sposób małoletni mogą uzyskać dostęp do danej usługi i korzystać z niej w sposób bezpieczny, dostosowany do wieku i chroniący ich prawa. Komisja jest zdania, że w razie stwierdzenia niezbędności potwierdzania wieku dla zagwarantowania wysokiego poziomu prywatności, bezpieczeństwa i ochrony, a także dla zapewnienia odpowiedniego do wieku doświadczenia, rejestracja lub uwierzytelnianie mogą stanowić pierwszy etap umożliwiający przeprowadzenie takiego procesu w sposób proporcjonalny.
55. W przypadku gdy rejestracja nie jest wymagana, mając na uwadze, że każdy niezarejestrowany użytkownik może być małoletnim poniżej wieku minimalnego wymaganego na platformie internetowej w celu uzyskania dostępu do usługi lub treści nieodpowiednich dla jego wieku udostępnianych w ramach usługi, dostawca odnośnej platformy internetowej dostępnej dla małoletnich powinien skonfigurować ustawienia wszelkich niezarejestrowanych użytkowników w sposób gwarantujący najwyższy poziom prywatności, bezpieczeństwa i ochrony, mając na względzie w szczególności zalecenia określone w sekcjach 6.3.1 i 6.3.2 i biorąc pod uwagę przede wszystkim najlepszy interes dziecka, w tym uwzględniając ryzyko związane z kontaktem z osobą dorosłą, która może podawać się za dziecko.
56. W przypadku gdy rejestracja jest wymagana lub oferowana jako możliwość do celów dostępu do platformy internetowej dostępnej dla małoletnich, Komisja uważa, że dostawca takiej platformy powinien:
 - a. Wyjaśnić użytkownikom, jakie są korzyści i zagrożenia związane z rejestracją oraz, w stosownych przypadkach, dlaczego rejestracja jest konieczna (zob. sekcja 8.4 dotycząca przejrzystości).
 - b. Zapewnić, aby proces rejestracji był dla wszystkich małoletnich łatwy pod względem dostępu i realizacji, odpowiednio do ich zmieniających się zdolności,

w tym dla osób z niepełnosprawnościami lub o dodatkowych potrzebach w zakresie dostępności, oraz aby był dostępny w zrozumiałym dla nich języku.

- c. Zapewnić, aby proces rejestracji obejmował środki pomagające użytkownikom zrozumieć, czy osiągnęli wystarczający wiek, aby móc korzystać z usługi. Zgodnie z lit. d) poniżej środki te powinny być przedstawiane użytkownikom dopiero po zastosowaniu metody potwierdzania wieku, w tym oświadczenia własnego.
- d. Unikać zachęcania lub nakłaniania użytkowników, którzy nie osiągnęli minimalnego wieku wymaganego na platformie internetowej dostępnej dla małoletnich, do tworzenia kont lub uzyskiwania dostępu do usługi, a także stosować środki mające na celu zmniejszenie ryzyka wystąpienia takiej sytuacji⁽⁵⁵⁾.
- e. Zapewnić, aby małoletni mogli z łatwością wylogować się i usunąć konto na żądanie.
- f. Wykorzystać w razie potrzeby proces rejestracji jako jedną z możliwości potwierdzenia wieku w świetle zaleceń zawartych w sekcjach 5 i 6.1⁽⁵⁶⁾, a także zwrócenia uwagi na zabezpieczenia platformy lub usługi, zasady postępowania oraz konsekwencje ich naruszenia, wszelkie zidentyfikowane zagrożenia dla prywatności, bezpieczeństwa lub ochrony małoletniego oraz zasoby dostępne do celów wsparcia użytkowników.
- g. Zapewnić, aby proces rejestracji nie zachęcał ani nie nakłaniał dzieci do udostępniania lub podawania na swoim profilu większej ilości informacji, niż jest to konieczne do funkcjonowania usługi, oraz aby konieczna była zgoda rodzica lub opiekuna dziecka w przypadkach, gdy jest wymagana na mocy prawa Unii lub prawa państwa członkowskiego.

⁽⁵⁵⁾ Pozostaje to bez uszczerbku dla dodatkowych wymogów wynikających z innych przepisów, takich jak art. 12 rozporządzenia (UE) 2016/679.

⁽⁵⁶⁾ Jak wspomniano w sekcji 6.1, Komisja nie uważa oświadczenia własnego za odpowiednią metodę potwierdzania wieku w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich zgodnie z art. 28 ust. 1 rozporządzenia (UE) 2022/2065.

6.3 Ustawienia konta

6.3.1 Ustawienia domyślne

57. Ustawienia domyślne to ważne narzędzie, którego dostawcy platform internetowych dostępnych dla małoletnich mogą używać w celu zmniejszania zagrożeń dla prywatności, bezpieczeństwa i ochrony małoletnich, takich jak np. ryzyko niepożądanego kontaktu ze strony osób działających na szkodę małoletnich. Dowody wskazują, że użytkownicy zazwyczaj nie zmieniają ustawień domyślnych, co oznacza, że w przypadku większości użytkowników ustawienia te pozostają bez zmian, a tym samym są kluczowe pod względem wpływu na zachowania ⁽⁵⁷⁾. Komisja uważa zatem, że dostawcy platform internetowych dostępnych dla małoletnich powinni:

- a. Zapewnić spójne stosowanie zasad prywatności, bezpieczeństwa i ochrony już w fazie projektowania w odniesieniu do wszystkich kont dla małoletnich.
- b. Domyślnie skonfigurować konta dla małoletnich w sposób gwarantujący najwyższy poziom prywatności, bezpieczeństwa i ochrony. Obejmuje to projektowanie ustawień domyślnych w taki sposób, aby zapewnić małoletnim bezpieczne i dostosowane do wieku ustawienia, z uwzględnieniem ich zmieniających się zdolności. Ustawienia te powinny zapewniać, aby w przypadku wszystkich małoletnich, w sposób domyślny, co najmniej:
 - i. konta umożliwiały interakcje takie jak polubienia, oznaczenia, komentarze, bezpośrednie wiadomości, udostępnianie i wzmianki tylko ze strony kont wcześniej zaakceptowanych przez użytkownika;

⁽⁵⁷⁾ Willis, L. E. (2014). Why not privacy by default? [Dlaczego nie domyślna ochrona prywatności?] *Berkeley Technology Law Journal*, 29(1), 61. Dostępne na stronie: https://www.btlj.org/data/articles2015/vol29/29_1/29-berkeley-tech-l-j-0061-0134.pdf; Cho, H., Roh, S., i Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings [Propagowanie tworzenia sieci kontaktów i ochrona prywatności: efekty ustawień domyślnych i regulacyjny nacisk na ustawienia preferencji użytkowników mediów społecznościowych]. *Computers in Human Behavior*, 101, 1–13. Dostępne na stronie: <https://doi.org/10.1016/j.chb.2019.07.001>. Przykłady ustawień, które mogą zagrażać prywatności, bezpieczeństwu lub ochronie małoletnich, to m.in. umożliwienie udostępniania lokalizacji, przełączanie się na profil publiczny, umożliwienie innym użytkownikom przeglądania list kontaktów lub list obserwujących, umożliwienie udostępniania plików medialnych oraz hosting lub udział w transmisji na żywo.

- ii. żadne konto nie mogło pobierać informacji ani wykonywać zrzutów ekranu zawierających informacje kontaktowe, dotyczące lokalizacji lub konta, ani treści zamieszczanych lub udostępnianych na platformie przez małoletnich;
- iii. tylko konta wcześniej zaakceptowane przez małoletniego mogły przeglądać umieszczane na jego koncie treści, wpisy i informacje o koncie;
- iv. nikt nie widział działań małoletniego, takich jak „polubienie” treści lub „obserwowanie” innego użytkownika;
- v. wyłączone były geolokalizacja, mikrofon, dostęp do zdjęć i kamera, synchronizacja kontaktów, a także wszystkie funkcje śledzenia, które nie są absolutnie niezbędne;
- vi. wyłączone było domyślne automatyczne odtwarzanie filmów wideo i hosting transmisji na żywo;
- vii. powiadomienia typu „push” były domyślnie wyłączone i zawsze wyłączone w najważniejszych godzinach snu, odpowiednich do wieku małoletniego. W przypadku gdy użytkownik aktywnie umożliwia wysyłanie powiadomień typu „push”, powinny one jedynie informować użytkownika o interakcjach z jego bezpośrednimi kontaktami oraz o treściach pochodzących z kont lub kanałów, które użytkownik aktywnie obserwuje lub z którymi wchodzi w interakcje (na przykład powiadomienia typu „push” nie powinny nigdy być nieautentyczne i zawsze powinny dokładnie wskazywać użytkownika lub twórcę, od którego pochodzi powiadomienie);
- viii. wyłączone były elementy, które mogą przyczyniać się do nadmiernego używania, takie jak liczniki „polubień” czy „reakcji”, „passy”, funkcja „...właśnie pisze” i „potwierdzenia odczytu”;
- ix. włączone były wszelkie funkcje, które wzmacniają sprawczość użytkowników w zakresie interakcji. Może to obejmować na przykład informacje lub elementy, które spowalniają wyświetlanie treści, ich zamieszczanie oraz interakcję z użytkownikami, dające użytkownikom możliwość zastanowienia się przed podjęciem decyzji o tym, czy chcą zobaczyć więcej treści lub zamieścić komentarz;

- x. wyłączone były rekomendacje dotyczące innych kont;
 - xi. wyłączone były filtry, które mogą powodować negatywne skutki od względem postrzegania własnego ciała, samooceny i zdrowia psychicznego.
- c. Przeanalizować, czy, w zależności od wieku i zmieniających się zdolności małoletnich oraz wyniku przeglądu ryzyka przeprowadzonego przez dostawcę, konieczne jest wyjście poza minimalne normy dotyczące ustawień domyślnych określone w niniejszej sekcji 6.3.1 oraz opracowanie i wdrożenie bardziej restrykcyjnych ustawień domyślnych. Może to np. dotyczyć opracowania domyślnych ustawień dla młodszych małoletnich, zgodnie z którymi żaden inny użytkownik nie może angażować się w określone rodzaje interakcji.
- d. Regularnie testować i aktualizować ustawienia domyślne, zapewniając ich skuteczność po każdej aktualizacji, także w odniesieniu do pojawiających się zagrożeń i tendencji w internecie, w tym wszelkich zagrożeń dla prywatności, bezpieczeństwa i ochrony małoletnich zidentyfikowanych przez dostawcę w trakcie przeglądu ryzyka (zob. sekcja 5 dotycząca przeglądu ryzyka).
- e. Zapewnić, aby małoletni nie byli w żaden sposób zachęcani ani nakłaniani do zmiany ustawień na niższy poziom prywatności, bezpieczeństwa i ochrony oraz aby wszelkie możliwości zmiany ustawień domyślnych były prezentowane w sposób neutralny.
- f. Zapewnić małoletnim rosnący poziom kontroli nad ustawieniami, odpowiednio do ich wieku, zmieniających się zdolności i potrzeb, w celu wspierania ich rosnącej autonomii i wzmacniania ich sprawczości ⁽⁵⁸⁾.
- g. Zapewnić, aby ustawienia były wyjaśniane małoletnim w sposób przyjazny i przystępny dla dzieci (zob. sekcja 6.4 dotycząca interfejsu internetowego i innych narzędzi).

⁽⁵⁸⁾ Małoletni przechodzą różne etapy rozwoju oraz wykazują różne poziomy dojrzałości i zrozumienia w zależności od wieku. Dostrzeżono to *m.in.* w komentarzu ogólnym nr 25 Komitetu Praw Dziecka ONZ w sprawie praw dzieci w odniesieniu do środowiska cyfrowego z 2021 r., pkt 19–21. Praktyczna tabela wieku i etapów rozwoju jest dostępna *m.in.* w załączniku do *Niderlandzkiego Kodeksu Dziecka*. Dostępne na stronie: <https://codevoorkinderrechten.waag.org/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf>

58. W przypadku gdy małoletni zmieniają ustawienia domyślne lub wybierają funkcje, które zagrażają ich prywatności, bezpieczeństwu lub ochronie, dostawca platformy internetowej, zdaniem Komisji, powinien:
- a. Umożliwić małoletnim dokonywanie wyboru między tymczasową zmianą ustawień domyślnych, na przykład na pewien okres lub do bieżącego wykorzystania w danej sesji, a trwałą zmianą tych ustawień.
 - b. Umożliwić łatwe przywrócenie ustawień domyślnych, np. za pomocą resetu jednym kliknięciem lub opartej na historii funkcji cofania w odniesieniu do ustawień, które zostały zmienione.
 - c. Wysyłać ostrzeżenia w momencie, w którym małoletni zmienia ustawienia, jasno wyjaśniając potencjalne konsekwencje zmian.
 - d. Regularnie przypominać małoletnim o potencjalnych konsekwencjach zmiany i regularnie umożliwiać im przywrócenie ustawień domyślnych.
 - e. Automatycznie wyłączać geolokalizację, mikrofon i kamerę, a także funkcje śledzenia, które nie są absolutnie niezbędne po zakończeniu sesji, jeżeli małoletni je wyłączył.
 - f. w przypadku włączenia geolokalizacji, mikrofonu i kamery musi to być widoczne dla małoletnich przez cały czas, w którym są funkcje te są włączone.

6.3.2 Dostępność ustawień, elementów i funkcji

59. Komisja uważa, że dostawcy platform internetowych dostępnych dla małoletnich powinni:
- a. Przeanalizować, czy niektórych ustawień, cech lub funkcji nie należy całkowicie usunąć z kont małoletnich lub czy któreś z ustawień domyślnych określonych w poprzedniej sekcji 6.3.1 nie powinny być niemożliwe do cofnięcia lub zmiany dla wszystkich małoletnich lub małoletnich w określonym wieku, z uwzględnieniem ich wieku i zmieniających się możliwości, oraz czy na podstawie tej oceny takie ustawienia nie powinny zostać usunięte lub nie powinny być niemożliwe do usunięcia. Dokonując tej oceny, dostawcy platform internetowych dostępnych dla małoletnich powinni wziąć pod uwagę, w jaki

sposób te ustawienia i funkcje mogą wpływać na wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich na ich platformie.

- b. Zapewnić, aby niezależnie od ustawień konta wybranych przez małoletnich:
 - i. małoletni nigdy nie mogli być z łatwością znajdowani przez konta, których wcześniej nie zaakceptowali jako kontaktów, ani konta takie nie powinny mieć możliwości łatwego kontaktowania się z nimi;
 - ii. osobistych danych kontaktowe małoletnich, w tym adresu e-mail lub numeru telefonu, nigdy nie ujawniano innym użytkownikom, chyba że małoletni wyraźnie na to zezwolił;
 - iii. kont małoletnich nigdy nie uwzględniano w sugestiach dotyczących kontaktów dla osób dorosłych. Konta dorosłych lub konta, które mogą należeć do osób dorosłych mogących podawać się za małoletnich nie powinny być rekomendowane małoletnim;
 - iv. konta, których małoletni nie zaakceptował wcześniej jako kontaktów, nigdy nie mogły zobaczyć jego danych profilowych, biogramu, działań i historii, w tym „polubień” i „wyświetleń”, listy znajomych i obserwujących oraz kont, które obserwuje małoletni, a także aby takie informacje zawsze stały się niedostępne, jeżeli dane konto zostanie zablokowane lub w inny sposób zostanie cofnięta jego akceptacja;
- c. zapewnić małoletnim możliwość ograniczenia widoczności ich zdjęć profilowych i poszczególnych publikowanych przez nich treści, a także możliwość ogólnego ograniczenia widoczności ich treści;
- d. zapewnić małoletnim możliwość akceptowania lub odrzucania wszelkich oznaczeń ze strony innych użytkowników, zarówno w treści, komentarzach, jak i w inny sposób;
- e. wdrożyć środki zapobiegające niezamierzonemu akceptowaniu przez małoletnich niepożądanych kontaktów, na przykład poprzez wymaganie od użytkowników, aby załączali wiadomość, kiedy wysyłają zaproszenie do kontaktu małoletniemu.

6.4 Projektowanie interfejsu internetowego i inne narzędzia

60. Komisja uważa, że środki umożliwiające małoletnim sprawowanie kontroli nad swoimi doświadczeniami w internecie stanowią skuteczny sposób zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich do celów art. 28 ust. 1 rozporządzenia (UE) 2022/2065.
61. Bez uszczerbku dla obowiązków dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych wynikających z rozdziału III sekcja 5 rozporządzenia (UE) 2022/2065 oraz niezależnie od obowiązków dostawców platform internetowych w zakresie projektu, organizacji i funkcjonowania ich interfejsów internetowych wynikających z art. 25 wspomnianego rozporządzenia, dostawcy platform internetowych dostępnych dla małoletnich, zdaniem Komisji, powinni przyjąć i wdrożyć funkcje umożliwiające małoletnim podejmowanie decyzji o sposobie korzystania ze świadczonych przez nich usług. Funkcje te powinny zapewniać właściwą równowagę między sprawczością dziecka a odpowiednim poziomem prywatności, bezpieczeństwa i ochrony. Powinno to obejmować na przykład:
 - a. Zapewnienie, aby projekt interfejsu internetowego oferował małoletnim odpowiednie do wieku doświadczenie.
 - b. Zapewnienie, aby małoletni nie byli narażeni na perswazyjne cechy projektu, które mają głównie na celu zaangażowanie i które mogą prowadzić do ekstensywnego lub nadmiernego korzystania z platformy lub do problematycznych bądź kompulsywnych nawyków behawioralnych. Cechy takie to m.in. możliwość przewijania w nieskończoność, zbędny wymóg wykonania określonego działania w celu otrzymania zaktualizowanych informacji w aplikacji, automatyczne uruchamianie treści wideo, powiadomienia celowo tak ustawione czasowo, żeby odwracać uwagę małoletnich, powiadomienia, które są nieautentyczne, w tym rzekomo pochodzące od innego użytkownika, lub powiadomienia społeczne o treściach, z którymi użytkownik nigdy nie miał styczności, informacje o niedoborze lub

pilności ⁽⁵⁹⁾ oraz tworzenie wirtualnych nagród za wykonywanie (powtarzanych) działań na platformie.

- c. Wprowadzenie zindywidualizowanych, widocznych, łatwo dostępnych, łatwych w użyciu, przyjaznych dziecku i skutecznych narzędzi zarządzania czasem, aby zwiększyć wśród małoletnich świadomość czasu spędzanego przez nich na platformach internetowych. Aby narzędzia te były skuteczne, powinny zniechęcać małoletnich do spędzania na platformie dłuższego czasu. Mogą się do nich również zaliczać łagodne sugestie wyboru bezpieczniejszych opcji. Należy również systematycznie wdrażać powiadomienia o aktywności, informujące małoletnich o czasie spędzonym w internecie.
- d. Zapewnienie, aby wszelkie narzędzia, cechy, funkcje, ustawienia, wskazówki, opcje i mechanizmy zgłaszania, przekazywania informacji zwrotnych i składania skarg były przyjazne dziecku, dostosowane do wieku, łatwo dostępne, łatwe do znalezienia, zrozumienia i użycia dla wszystkich małoletnich, w tym osób z niepełnosprawnościami lub dodatkowymi potrzebami w zakresie dostępności, oraz aby nie wymagały zmiany urządzeń w celu przeprowadzenia jakichkolwiek działań.
- e. Zapewnienie, aby w przypadku gdy z platformą internetową dostępną dla małoletnich zintegrowane są funkcje sztucznej inteligencji, takie jak chatboty i filtry AI, nie były one uruchamiane automatycznie, a małoletni nie byli zachęcani ani nakłaniani do korzystania z nich oraz aby takie systemy odpowiadały zmieniającym się możliwościom małoletnich i były zaprojektowane w sposób dla nich bezpieczny. W związku z tym Komisja uważa, że funkcje AI powinny być udostępniane na platformach internetowych dostępnych dla małoletnich dopiero po dokonaniu oceny ryzyka, które te elementy AI mogą stwarzać dla prywatności, bezpieczeństwa i ochrony małoletnich, oraz że powinny być one łatwe do wyłączenia i powinno być jasne, kiedy nie są wyłączone.

⁽⁵⁹⁾ Komisja przypomina, że dyrektywa 2005/29/WE zakazuje nieuczciwych praktyk handlowych, w tym, w załączniku I pkt 7, fałszywych twierdzeń, że produkt będzie dostępny jedynie przez ograniczony czas lub że będzie on dostępny na określonych warunkach przez bardzo ograniczony czas, w celu nakłonienia konsumentów do podjęcia natychmiastowej decyzji i pozbawienia ich możliwości świadomego wyboru lub czasu potrzebnego do jego dokonania.

- f. Zapewnienie wdrożenia środków technicznych mających na celu ostrzeżenie⁽⁶⁰⁾ małoletnich, że interakcje z elementem AI różnią się od interakcji międzyludzkich oraz że elementy te mogą podawać informacje, które są niezgodne ze stanem faktycznym i mogą wprowadzać w błąd. Ostrzeżenie to powinno być łatwo widoczne, sformułowane w sposób przyjaznym dziecku i bezpośrednio dostępne z interfejsu oraz przez cały czas interakcji małoletniego z elementem AI. Na przykład chatboty AI nie powinny być eksponowane w sposób rzucający się w oczy, nie powinny być częścią sugerowanych kontaktów ani grup użytkowników, z którymi małoletni jest w kontakcie. Dostawcy platform internetowych powinni zapewnić, aby małoletni i ich opiekunowie mieli możliwość rezygnacji z korzystania z chatbotów AI oraz aby nie nakłaniano ich do korzystania z tych funkcji⁽⁶¹⁾. Takie elementy AI nie mogą być wykorzystywane do wywierania wpływu na małoletnich ani do nakłaniania ich do korzystania z treści komercyjnych lub do zakupów.

Złe praktyki

SadFriends to platforma społecznościowa, na której profile małoletnich podlegają tym samym ustawieniom, co profile osób dorosłych. Po rejestracji informacje o kontaktach małoletnich i zamieszczane przez nich treści są widoczne dla innych użytkowników na platformie i poza nią. Z małoletnimi mogą kontaktować się inni użytkownicy, którzy nie zostali przez nich zaakceptowani jako kontakty. Tacy użytkownicy mogą wysłać do małoletnich wiadomości i komentować ich treści. Gdy małoletni włącza geolokalizację, aby udostępnić swoją lokalizację znajomym, staje się ona widoczna dla wszystkich kont, które znajdują się na jego liście znajomych, i pozostaje widoczna po zamknięciu sesji, co oznacza, że inni użytkownicy widzą, gdzie się znajduje, dopóki małoletni nie przypomni sobie o wyłączeniu geolokalizacji.

W rezultacie podmioty działające w złych zamiarach zaczynają atakować małoletnich na SadFriends. Nieznane osoby dorosłe docierają do małoletnich i kontaktują się z nimi, budując więzi emocjonalne i uzyskując ich zaufanie. Małoletni są nagabywani w celach seksualnych i zmuszani do tworzenia obrazów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych oraz do udostępniania ich innym osobom.

⁽⁶⁰⁾ Komisja przypomina, że dostawcy systemów AI, które są przeznaczone do wchodzenia w bezpośrednią interakcję z osobami fizycznymi, mają obowiązek zapewnienia, aby były one projektowane i opracowywane w taki sposób, aby zainteresowane osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem AI zgodnie z art. 50 ust. 1 rozporządzenia (UE) 2024/1689 („akt w sprawie sztucznej inteligencji”). Wszelkie środki wprowadzone zgodnie z niniejszym zaleceniem należy rozumieć zgodnie ze środkami wprowadzonymi w celu zapewnienia zgodności z art. 50 ust. 1 aktu w sprawie sztucznej inteligencji, w tym z przewidzianym w nim systemem nadzoru i egzekwowania, a także bez uszczerbku dla tych środków.

⁽⁶¹⁾ Komisja przypomina o wytycznych w sprawie zakazanych praktyk w zakresie sztucznej inteligencji określonych w rozporządzeniu (UE) 2024/1689 (akt w sprawie sztucznej inteligencji).

6.5 Systemy rekomendacji i funkcje wyszukiwania

62. Systemy rekomendacji ⁽⁶²⁾ określają, w jaki sposób informacje są szeregowane, optymalizowane i prezentowane małoletnim. W rezultacie takie systemy mają istotny wpływ na to, czy i w jakim stopniu małoletni napotykają w internecie określone rodzaje treści, kontaktów lub zachowań. Systemy rekomendacji mogą stwarzać i pogłębiać zagrożenia dla prywatności, bezpieczeństwa i ochrony małoletnich w internecie, na przykład wzmacniając treści, które mogą mieć negatywny wpływ na bezpieczeństwo i ochronę małoletnich ⁽⁶³⁾.
63. Komisja przypomina o obowiązkach dotyczących przejrzystości systemów rekomendacji spoczywających na wszystkich dostawcach wszystkich kategorii platform internetowych na podstawie art. 27 rozporządzenia (UE) 2022/2065 oraz o dodatkowych wymogach w tym zakresie dotyczących dostawców bardzo dużych

⁽⁶²⁾ Do celów niniejszej sekcji Komisja przypomina, że zgodnie z art. 3 lit. s) rozporządzenia (UE) 2022/2065 systemy rekomendacji obejmują systemy wdrożone do celów rekomendacji dotyczących treści, produktów, reklam, kontaktów, autouzupełniania w wyszukiwarkach i wyników wyszukiwania.

⁽⁶³⁾ Munn, L. (2020). Angry by design: Toxic communication and technical architectures [Gniew w fazie projektowania: toksyczna komunikacja i architektura techniczna]. *Humanities and Social Sciences Communications*, 7(53). Dostępne na stronie: <https://doi.org/10.1057/s41599-020-00550-7>; Milli, S. i in. (2025). Engagement, user satisfaction, and the amplification of divisive content on social media [Zaangażowanie, zadowolenie użytkowników i szerzenie w mediach społecznościowych treści prowadzących do podziałów]. *PNAS Nexus*, 4(3) pgaf062. Dostępne na stronie: <https://doi.org/10.1093/pnasnexus/pgaf062>; Piccardi, T. i in. (2024). Social Media Algorithms Can Shape Affective Polarization via Exposure to Antidemocratic Attitudes and Partisan Animosity [Algorytmy mediów społecznościowych mogą kształtować afektywną polaryzację poprzez ekspozycję na postawy antydemokratyczne i animozje międzypartyjne]. Dostępne na stronie: [10.48550/arXiv.2411.14652](https://arxiv.org/abs/2411.14652); Harriger, J. A., Evans, J. L., Thompson, J. K. i Tylka, T. L. (2022). The dangers of the rabbit hole: Reflections on social media as a portal into a distorted world of edited bodies and eating disorder risk and the role of algorithms [Zagrożenia króliczej nory: refleksje na temat mediów społecznościowych jako portalu do zniekształconego świata zmanipulowanych ciał i ryzyka zaburzeń odżywiania oraz roli algorytmów]. *Body Image*, 41, 292–297. Dostępne na stronie: <https://doi.org/10.1016/j.bodyim.2022.03.007>; Amnesty International (2023). Driven into darkness: How TikTok's 'For You' feed encourages self-harm and suicidal ideation [Wpędzani w ciemność: jak funkcja „Dla ciebie” w serwisie TikTok zachęca do samookaleczeń i myśli samobójczych]. Dostępne na stronie: <https://www.amnesty.org/en/documents/pol40/7350/2023/en/>; Hilbert, M., Ahmed, S., Cho, J. i Chen, Y. (2024). #BigTech @Minors: Social media algorithms quickly personalize minors' content, lacking equally quick protection [Wielkie firmy technologiczne i małoletni: algorytmy mediów społecznościowych szybko personalizują treści osób niepełnoletnich, bez równie szybkiej ochrony]. Dostępne na stronie: [http://dx.doi.org/10.2139/ssrn.4674573](https://dx.doi.org/10.2139/ssrn.4674573); Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review [Korzystanie z mediów społecznościowych a zdrowie psychiczne i dobrostan młodzieży: przegląd ogólny], *Computers in Human Behavior Reports*, t. 14, 100404, ISSN 2451-9588. Dostępne na stronie: <https://doi.org/10.1016/j.chbr.2024.100404>.

platform internetowych i bardzo dużych wyszukiwarek internetowych określonych w art. 34 ust. 1, art. 35 ust. 1 i art. 38 rozporządzenia (UE) 2022/2065 ⁽⁶⁴⁾.

64. Komisja uważa, że w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony, w szczególności w odniesieniu do małoletnich, zgodnie z wymogami art. 28 ust. 1 rozporządzenia (UE) 2022/2065, dostawcy platform internetowych dostępnych dla małoletnich powinni wprowadzić następujące środki:

6.5.1 Testowanie i dostosowywanie budowy i funkcjonowania systemów rekomendacji dla małoletnich

65. Dostawcy platform internetowych dostępnych dla małoletnich, którzy w związku ze świadczeniem usługi korzystają z systemów rekomendacji, powinni:
- a. Regularnie testować i dostosowywać swoje systemy rekomendacji w celu zwiększenia prywatności, bezpieczeństwa i ochrony małoletnich oraz zgodnie z wynikami przeglądu ryzyka, o którym mowa w sekcji 5, obejmującego uwzględnienie szerszych praw dziecka. Takie testy i dostosowania powinny odbywać się w porozumieniu z małoletnimi, opiekunami i niezależnymi ekspertami.
 - b. Przy określaniu celów, parametrów i strategii oceny systemów rekomendacji uwzględniać szczególne potrzeby, cechy charakterystyczne, niepełnosprawność i dodatkowe potrzeby małoletnich w zakresie dostępności, również z należytym uwzględnieniem ich grupy wiekowej. Priorytetowo należy traktować parametry i mierniki związane z dokładnością, różnorodnością, inkluzywnością i sprawiedliwością.
 - c. Zapewnić, aby systemy rekomendacji nie gromadziły żadnych danych behawioralnych obejmujących działania małoletniego poza platformą.
 - d. Zapewnić, aby w przypadku gdy system rekomendacji opiera się na przetwarzaniu danych behawioralnych dotyczących małoletniego, sugestie dotyczące konkretnych informacji dla małoletnich odbiorców usługi lub uszeregowanie tych informacji nie opierały się na przetwarzaniu behawioralnych

⁽⁶⁴⁾ Komisja przypomina również, że inne przepisy unijne lub krajowe mogą wpływać na projektowanie i funkcjonowanie systemów rekomendacji ze względów zapewnienia ochrony interesów prawnych wchodzących w ich zakres, co przyczynia się do wysokiego poziomu prywatności, bezpieczeństwa i ochrony praw podstawowych w internecie.

danych osobowych o zakresie tak szerokim, że obejmuje wszystkie działania lub większość działań małoletniego na platformie, co może wywoływać poczucie, że życie prywatne małoletniego jest stale monitorowane.

- e. Zapewnić, aby systemy rekomendacji opierały się na „domyślnych sygnałach opartych na zaangażowaniu” dopiero po dokonaniu oceny, czy leży to w najlepszym interesie małoletniego, z uwzględnieniem zasad minimalizacji danych i przejrzystości, oraz pod warunkiem, że takie wykorzystanie jest jasno zdefiniowane i podlega odpowiednim zabezpieczeniom dokładniej określonym w powyższych zaleceniach.
- f. Do celów niniejszych wytycznych termin „domyślne sygnały oparte na zaangażowaniu” należy rozumieć jako odnoszący się do sygnałów i danych, które umożliwiają wnioskowanie o preferencjach użytkowników na podstawie ich działań (zachowanie na platformie), np. czasu poświęconego na oglądanie treści i współczynników klikalności.
- g. Traktować priorytetowo „wyraźne sygnały ze strony użytkownika” w celu określania, jakie treści mają być prezentowane i rekomendowane małoletnim. Wybór takich sygnałów powinien być uzasadniony najlepszym interesem małoletniego, z uwzględnieniem zasad minimalizacji danych i przejrzystości, co pomoże zapewnić, aby sygnały te przyczyniały się do wysokiego poziomu bezpieczeństwa i ochrony małoletnich. Do celów niniejszych wytycznych termin „wyraźne sygnały ze strony użytkownika” należy rozumieć jako odnoszący się do informacji zwrotnych od użytkowników i interakcji, które wskazują na wyraźne preferencje użytkowników, zarówno pozytywne, jak i negatywne, w tym określony i deliberatywny wybór tematów będących przedmiotem zainteresowania, ankiet, zgłoszeń ⁽⁶⁵⁾ i innych sygnałów o charakterze jakościowym.

⁽⁶⁵⁾ Przykładowo, w rankingu systemów rekomendacji należy uwzględnić informacje zwrotne od małoletnich na temat treści, działań, osób, kont lub grup, które wywołują u nich poczucie dyskomfortu lub z którymi chcą mieć więcej lub mniej styczności. Mogą to być informacje zwrotne takie jak: „Pokaż mniej/więcej”, „Nie chcę widzieć/nie jestem zainteresowany(-a)”, „Nie chcę widzieć treści z tego konta”, „To powoduje u mnie dyskomfort”, „Ukryj to”, „Nie lubię tego” lub „To nie dla mnie”. Zob. także sekcja 7.1 niniejszych wytycznych dotycząca zgłoszeń użytkowników, informacji zwrotnych i skarg.

- h. Wdrożyć środki mające na celu zapobieganie narażeniu małoletnich na rekomendacje dotyczące treści, które mogłyby stanowić zagrożenie dla ich bezpieczeństwa i ochrony, w szczególności w przypadku ponownego napotkania, takich jak treści propagujące nierealistyczne normy piękna lub diety, treści gloryfikujące lub trywializujące problemy ze zdrowiem psychicznym, takie jak lęki czy depresja, treści dyskryminujące, treści powodujące radykalizację i wywołujące niepokój treści przedstawiające przemoc lub zachęcające małoletnich do angażowania się w niebezpieczne działania. Obejmuje to treści zgłoszone lub oznaczone przez użytkowników, zaufane podmioty sygnalizujące lub inne podmioty lub narzędzia moderowania treści, których zgodność z prawem i z warunkami korzystania z usług platformy nie została jeszcze zweryfikowana, na mocy odpowiednich zobowiązań wynikających z rozporządzenia (UE) 2022/2065 i sekcji 6.7.
- i. Wdrożyć środki w celu zapewnienia, aby systemy rekomendacji nie umożliwiały ani nie ułatwiały rozpowszechniania nielegalnych treści lub popełniania przestępstw przeciwko małoletnim i przez małoletnich.
- j. Zapewnić, aby w wynikach wyszukiwania i sugestjach dotyczących kontaktów dla małoletnich priorytetowo traktowano konta, których tożsamość została zweryfikowana, a także kontakty należące do sieci małoletniego lub kontakty w tym samym przedziale wiekowym, co małoletni.
- k. Zapewnić, aby funkcje wyszukiwania, w tym m.in. autouzupełnianie tekstu na pasku wyszukiwania oraz sugerowane terminy i kluczowe wyrażenia, nie rekomendowały treści, które są nielegalne lub kwalifikują się jako szkodliwe dla prywatności, bezpieczeństwa lub ochrony małoletnich, na przykład poprzez blokowanie haseł wyszukiwania, o których dobrze wiadomo, że aktywują treści uznawane za szkodliwe dla prywatności, bezpieczeństwa lub ochrony małoletnich, takich jak konkretne słowa, wyrażenia slangowe, hashtagi lub emotikony ⁽⁶⁶⁾. W przypadku zapytań związanych z takimi treściami dostawcy

⁽⁶⁶⁾ Przykładowe hasła można znaleźć w pakiecie wiedzy w zakresie zwalczania sprzedaży narkotyków w internecie, który opracowano w ramach Forum UE ds. Internetu i który zawiera ponad 3 500 haseł, emotikonów i wyrażen slangowych używanych przez handlarzy narkotyków do celów sprzedaży narkotyków w internecie – zob. odniesienie w unijnym planie działania na rzecz zwalczania nielegalnego obrotu środkami odurzającymi i przestępczości zorganizowanej, COM(2023) 641 final.

platform internetowych powinni przekierowywać małoletnich do odpowiednich zasobów wsparcia i telefonów zaufania.

6.5.2 Kontrola ze strony użytkowników i wzmocnienie ich pozycji

66. Korzystający z systemów rekomendacji dostawcy platform internetowych dostępnych dla małoletnich powinni, świadcząc swoje usługi, przyjąć następujące środki w celu zagwarantowania wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich:
- a. Zapewnić małoletnim możliwość całkowitego i trwałego resetowania swoich list rekomendacji.
 - b. W ramach ustalania priorytetów dotyczących parametrów i wskaźników związanych z dokładnością, różnorodnością, inkluzywnością i sprawiedliwością udostępniać małoletnim informacje i zachęcać ich do poszukiwania nowych treści po pewnej ilości interakcji z systemem rekomendacji.
 - c. Ocenić, czy ze względu na szczególne cechy platformy oraz w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich na takiej platformie właściwe jest zagwarantowanie małoletnim możliwości wyboru opcji systemu rekomendacji, która nie jest oparta na profilowaniu. Niniejsze zalecenie pozostaje bez uszczerbku dla obowiązków dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych wynikających z art. 38 rozporządzenia (UE) 2022/2065.
 - d. W przypadku gdy w wyniku oceny, o której mowa w powyższym punkcie, lub w wyniku wypełniania obowiązków wynikających z art. 38 rozporządzenia (UE) 2022/2065, spoczywających na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, wprowadzili oni opcję systemu rekomendacji, która nie opiera się na profilowaniu, ocenić, czy należy ją skonfigurować jako ustawienie domyślne oraz, jeśli uznają to za właściwe, wprowadzić niezbędne zabezpieczenia i środki na rzecz przejrzystości w celu informowania małoletnich o takiej opcji i potencjalnych konsekwencjach wyłączenia takiego ustawienia domyślnego.
 - e. Zapewnić, aby odpowiednie mechanizmy zgłaszania i przekazywania informacji zwrotnych określone w sekcji 7.1 miały szybki, bezpośredni i trwały wpływ na

parametry systemów rekomendacji, ich edytowanie i wyniki przez nie prezentowane. Obejmuje to trwałe usuwanie z zaleceń zgłoszonych treści i kontaktów (w tym treści zgłoszonych do ukrycia i zablokowanych/zgłoszonych kontaktów) oraz zmniejszenie widoczności podobnych treści i kont.

67. Komisja uważa, że oprócz wypełniania obowiązków określonych w art. 27 ust. 1 rozporządzenia (UE) 2022/2065 oraz, w odniesieniu do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, wzmocnionych obowiązków w zakresie należytej staranności określonych w art. 34, 35 i 38 wspomnianego rozporządzenia, dostawcy platform internetowych dostępnych dla małoletnich powinni:

- a. Zapewnić, aby wszelkie ustawienia i informacje przekazywane małoletnim na temat systemów rekomendacji, w tym m.in. warunki korzystania z usług, były prezentowane w sposób przyjazny dziecku i dostępny, dostosowany do wieku i zmieniającej się dojrzałości dziecka oraz w zrozumiałym dla niego języku (więcej szczegółowych informacji można znaleźć w sekcji 6.4 dotyczącej projektowania interfejsu internetowego i innych narzędzi oraz w sekcji 8.4 dotyczącej przejrzystości).
- b. W zrozumiały sposób wyjaśniać, dlaczego zalecana jest każda konkretna treść, w tym z podaniem informacji na temat zastosowanych parametrów i sygnałów użytkownika zgromadzonych do celów danej rekomendacji.
- c. Udostępniać małoletnim, w sposób przystępny, z zastosowaniem sformułowań i projektu przyjaznych dziecku, opcje zmiany parametrów systemów rekomendacji lub wpływania na takie parametry, na przykład poprzez umożliwienie im wyboru kategorii treści i działań, którymi są najbardziej lub najmniej zainteresowani, z podaniem wyjaśnień sformułowanych w sposób zrozumiały dla dzieci. Opcje te powinny być oferowane przy tworzeniu konta i regularnie przez cały czas pobytu małoletniego na platformie. Preferencje te powinny mieć bezpośredni wpływ na rekomendacje przedstawiane przez system, zapewniając ich ściślejsze dostosowanie do wieku i najlepszego interesu małoletniego ⁽⁶⁷⁾.

⁽⁶⁷⁾ Zob. art. 27 ust. 1 i 3 rozporządzenia (UE) 2022/2065.

6.6 Praktyki handlowe

68. Małoletni są szczególnie narażeni na perswazyjne skutki praktyk handlowych i mają prawo do ochrony przed praktykami wyzysku ekonomicznego⁽⁶⁸⁾ stosowanymi przez platformy internetowe. Mają oni do czynienia ze stosowanymi przez platformy internetowe praktykami handlowymi wykorzystującymi różnorodne, dynamiczne i spersonalizowane metody perswazji, na przykład poprzez reklamę, lokowanie produktu, stosowanie walut wewnątrz aplikacji, praktyki marketingowe influencerów, sponsorowanie czy zachęty wzmacniane przez AI⁽⁶⁹⁾ ⁽⁷⁰⁾. Może to mieć negatywny wpływ na prywatność, bezpieczeństwo i ochronę małoletnich korzystających z usług platformy internetowej.
69. Komisja uważa, że zgodnie z obowiązującymi horyzontalnymi ramami prawnymi, w szczególności z dyrektywą 2005/29/WE o nieuczciwych praktykach handlowych, która ma pełne zastosowanie do wszystkich praktyk handlowych, również wobec małoletnich⁽⁷¹⁾, a także z bardziej szczegółowymi przepisami rozporządzenia (UE) 2022/2065 w sprawie reklamy (art. 26, art. 28 ust. 2 i art. 39) i zwodniczych interfejsów (art. 25) oraz bez uszczerbku dla tych przepisów dostawcy platform

⁽⁶⁸⁾ Komitet Praw Dziecka, komentarz ogólny nr 25, pkt 112; UNICEF (2019). Discussion paper: Digital marketing and children's rights [Dokument otwierający debatę: marketing cyfrowy i prawa dziecka]. Dostępne na stronie: <https://www.unicef.org/childrightsandbusiness/media/256/file/Discussion-Paper-Digital-Marketing.pdf>.

⁽⁶⁹⁾ Z tego względu doświadczają trudności np. z rozróżnianiem między treściami o charakterze komercyjnym i niekomercyjnym, z przeciwstawianiem się presji rówieśniczej na zakup treści w grze lub w aplikacji, które są atrakcyjne dla małoletnich lub wręcz niezbędne do osiągnięcia postępów w grze, ze zrozumieniem rzeczywistej wartości walut w aplikacjach lub faktu, że w randomizowanych zakupach w aplikacji lub w grze najbardziej pożądane treści, takie jak aktualizacje, mapy i awatary, mogą występować rzadziej niż treści mniej pożądane.

⁽⁷⁰⁾ M. Ganapini, E. Panai (2023) *An Audit Framework for Adopting AI-Nudging on Children* [Ramy kontroli stosowania sztucznej inteligencji w celu wywierania wpływu na dzieci]. Dostępne na stronie: <https://arxiv.org/pdf/2304.14338>

⁽⁷¹⁾ Komisja przypomina, że zgodnie z art. 2 ust. 4 rozporządzenia (UE) 2022/2065 pozostaje ono bez uszczerbku dla dyrektywy 2010/13/UE, prawa Unii dotyczącego prawa autorskiego i praw pokrewnych, rozporządzenia (UE) 2021/784, rozporządzenia (UE) 2019/1148, rozporządzenia (UE) 2019/1150, prawa Unii dotyczącego ochrony konsumentów i bezpieczeństwa produktów (w tym dyrektywy (UE) 2005/29) i prawa Unii dotyczącego ochrony danych osobowych, prawa Unii w dziedzinie współpracy sądowej w sprawach cywilnych, prawa Unii w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych oraz dyrektywy ustanawiającej zharmonizowane przepisy dotyczące wyznaczania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych. Ponadto nie wpływa ono na stosowanie dyrektywy 2000/31/WE. Zgodnie z art. 91 rozporządzenia (UE) 2022/2065 Komisja jest upoważniona do przeprowadzenia oceny i przedstawienia do dnia 17 listopada 2025 r. sprawozdania na temat relacji między tym rozporządzeniem a innymi aktami prawnymi, w szczególności aktami, o których mowa powyżej.

internetowych dostępnych dla małoletnich powinni przyjąć następujące środki w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich korzystających ze świadczonych przez nich usług do celów art. 28 ust. 1 rozporządzenia (UE) 2022/2065:

- a. Zapewnić, aby brak wiedzy w dziedzinie handlu wśród małoletnich nie był wykorzystywany, biorąc pod uwagę wiek małoletnich, ich podatność na zagrożenia i ograniczoną zdolność do krytycznego angażowania się w praktyki handlowe na platformie, a także udzielać odpowiedniego wsparcia ⁽⁷²⁾.
- b. Zapewnić, aby małoletni nie byli narażeni na szkodliwą, nieetyczną i niezgodną z prawem reklamę ⁽⁷³⁾. Może to obejmować na przykład rozważenie stosowności kampanii reklamowych kierowanych do poszczególnych grup wiekowych, uwzględnienie niekorzystnych skutków takich kampanii oraz podjęcie odpowiednich środków bezpieczeństwa w celu ochrony małoletnich, a także zapewnienia im dostępu do informacji, które najlepiej odpowiadają ich interesom ⁽⁷⁴⁾.
- c. Regularnie dokonywać przeglądu odpowiednich środków ochronnych w porozumieniu z małoletnimi, opiekunami i innymi odpowiednimi zainteresowanymi stronami.
- d. Zapewnić, aby małoletni nie byli narażeni na nadmierne łączne ilości i nadmierną częstotliwość prezentowania treści komercyjnych oraz nadmierne rekomendacje dotyczące takich treści, które mogą prowadzić do nadmiernych

⁽⁷²⁾ UNICEF zapewnia zasoby i wytyczne dla platform dotyczące ekosystemu marketingu cyfrowego, w tym dokument UNICEF (2025) *Discussion Paper on digital marketing and children's rights* [Dokument otwierający debatę na temat marketingu cyfrowego i praw dziecka], dostępny pod adresem <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/digital-marketing>.

⁽⁷³⁾ Komisja przypomina, że np. przedsiębiorcy podlegają na podstawie art. 5 ust. 1 dyrektywy 2005/29/WE zakazowi dopuszczania się nieuczciwych praktyk handlowych, a pkt 28 załącznika I do tej dyrektywy zakazuje bezpośredniego wzywania dzieci do nabycia reklamowanych produktów lub nakłaniania do tego rodziców lub innych osób dorosłych. Takie zachowanie handlowe w każdych okolicznościach uznaje się za nieuczciwe.

⁽⁷⁴⁾ Komentarz ogólny Komitetu Praw Dziecka nr 25 (2021) w sprawie praw dziecka w środowisku cyfrowym stanowi, że najlepszy interes dziecka powinien być „najważniejszym aspektem regulacji dotyczących reklamy i marketingu skierowanych do dzieci i dostępnych dla dzieci. Sponsorowanie, lokowanie produktu i wszelkie inne rodzaje treści o charakterze komercyjnym powinny być wyraźnie odróżniane od wszelkich innych treści i nie powinny utrzymywać stereotypów związanych z płcią lub rasą”.

lub niepożądanych wydatków lub zachowań nałogowych, a także mieć szkodliwy wpływ na prywatność, bezpieczeństwo i ochronę małoletnich.

- e. Zapewnić, aby małoletni nie byli narażeni na zintegrowane z platformą systemy AI, które wywierają na dzieci wpływ lub stymulują je w celach komercyjnych, w szczególności poprzez formaty konwersacyjne lub doradcze, takie jak chatboty ⁽⁷⁵⁾.
- f. Zapewnić, aby oświadczenia o handlowym charakterze informacji były wyraźnie widoczne, przyjazne dziecku, dostosowane do wieku i dostępne (zob. sekcja 8.4 dotycząca przejrzystości) oraz wykorzystywane w sposób spójny w całej usłudze, na przykład przez umieszczanie ikony lub podobnego znaku w celu wyraźnego wskazania, że treści są reklamami ⁽⁷⁶⁾. Oznaczenia takie powinny być regularnie testowane i poddawane przeglądowi w porozumieniu z małoletnimi, ich opiekunami i innymi odpowiednimi zainteresowanymi stronami.
- g. Zapewnić, aby małoletni nie byli narażeni na marketing i komunikację na temat produktów lub usług, które mogą mieć negatywny wpływ na ich prywatność, bezpieczeństwo i ochronę, w tym produktów lub usług określonych w przeglądzie ryzyka przeprowadzonym przez dostawcę, np. związanych z negatywnym wpływem na zdrowie fizyczne i psychiczne małoletnich (zob. sekcja 5 dotycząca przeglądu ryzyka).
- h. Zapewnić, aby małoletni nie byli narażeni na ukrytą lub zakamuflowaną reklamę, bez względu na to, czy jest ona zamieszczana przez dostawcę platformy

⁽⁷⁵⁾ Komisja przypomina, że takie użycie systemów sztucznej inteligencji może stanowić zakazaną praktykę w świetle art. 5 ust. 1 lit. b) rozporządzenia (UE) 2024/1689, jeżeli wykorzystują słabości dzieci w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić poważną szkodę. Wszelkie środki wprowadzane zgodnie z niniejszym zaleceniem powinny wykraczać poza środki wprowadzane w celu uniemożliwienia stosowania tego zakazu. Nadzór nad środkami wprowadzonymi w celu zapewnienia zgodności z art. 50 ust. 1 rozporządzenia (UE) 2024/1689 i egzekwowanie tych środków pozostają w gestii właściwych organów na podstawie wspomnianego rozporządzenia.

⁽⁷⁶⁾ Komisja przypomina, że zgodnie z art. 6 i 7 dyrektywy 2005/29/WE ujawnienie elementu handlowego musi być jasne i odpowiednie i należy w nim uwzględnić środek przekazu, za pośrednictwem którego odbywa się marketing, w tym kontekst, lokowanie, harmonogram, czas trwania, język czy grupę docelową. Zob. również [Wytyczne dotyczące wykładni i stosowania dyrektywy 2005/29/WE](#).

internetowej, czy przez użytkowników usługi ⁽⁷⁷⁾. W tym kontekście Komisja przypomina, że dostawcy platform internetowych są również zobowiązani, zgodnie z art. 26 ust. 2 rozporządzenia (UE) 2022/2065, do zapewnienia odbiorcom usługi funkcji umożliwiającej składanie oświadczenia, czy przekazywane przez nich treści są informacjami handlowym lub zawierają informacje handlowe ⁽⁷⁸⁾. Przykładami ukrytych informacji handlowych mogą być m.in. lokowanie produktu przez influencerów, prezentacje produktów i inne formy zawoalowanej promocji, które mogą wprowadzać małoletnich w błąd lub manipulować nimi, nakłaniając ich do zakupu produktów lub usług.

- i. Zapewnić, aby dzieci nie były narażone na techniki, które mogą skutkować ograniczeniem przejrzystości transakcji gospodarczych oraz wprowadzać w błąd małoletnich – dotyczy to np. niektórych walut wirtualnych ⁽⁷⁹⁾ oraz innych tokenów lub monet, które mogą być wymieniane na realne pieniądze (lub, w stosownych przypadkach, służyć do zakupu innej waluty wirtualnej) i wykorzystywane do zakupu przedmiotów wirtualnych, a tym samym powodują niepożądane wydatki ⁽⁸⁰⁾.
- j. Zapewnić, aby małoletnim uzyskującym dostęp do platform internetowych lub ich części i elementów, które są prezentowane jako bezpłatne lub sprawiają takie wrażenie ⁽⁸¹⁾, nie podsuwano możliwości dokonywania zakupów w aplikacji lub

⁽⁷⁷⁾ Komisja przypomina, że w art. 7 ust. 2 dyrektywy 2005/29/WE oraz w załączniku I pkt 22 zakazuje się fałszywego twierdzenia lub stwarzania wrażenia, że sprzedawca nie działa w celu związanym z jego działalnością handlową, gospodarczą, rzemieślniczą lub wolnym zawodem lub fałszywego podawania się za konsumenta. Przypomina również o dyrektywie 2010/13/UE, która zakazuje bezpośredniego nakłaniania małoletnich do kupna lub najmu produktu lub usługi, zachęcania ich do przekonywania rodziców lub osób trzecich do kupna reklamowanych produktów lub usług, a także wykorzystywania szczególnego zaufania, którym małoletni darzą rodziców, nauczycieli lub inne osoby. Zgodnie z motywem 10 rozporządzenia 2022/2065 rozporządzenie to powinno pozostawać bez uszczerbku dla prawa Unii dotyczącego ochrony konsumentów, w tym dyrektywy 2005/29 dotyczącej nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym.

⁽⁷⁸⁾ Komisja przypomina również, że zgodnie z dyrektywą 2010/13/UE platformy udostępniania wideo muszą posiadać funkcję umożliwiającą zadeklarowanie, że zamieszczane treści zawierają handlowe przekazy audiowizualne.

⁽⁷⁹⁾ Komisja przypomina, że pojęcie waluty wirtualnej zdefiniowano w dyrektywie (UE) 2018/843 w sprawie przeciwdziałania praniu pieniędzy.

⁽⁸⁰⁾ Przykład zastosowany w niniejszym zaleceniu jest nieistotny w odniesieniu do jakiegokolwiek klasyfikacji prawnej lub definicji walut w grach w obowiązującym prawie Unii lub jego interpretacji związanej ze skutkami stosowania takich instrumentów.

⁽⁸¹⁾ Komisja przypomina, że w pkt 20 załącznika I do dyrektywy 2005/29/WE zakazuje się opisywania produktu jako „gratis”, „darmowy”, „bezpłatny” lub w podobny sposób, jeżeli konsument musi uiścić jakąkolwiek inną należność niż nieunikniony koszt związany z odpowiedzią na praktykę handlową, odbiorem lub dostarczeniem produktu.

w grze, które są lub wydają się niezbędne w celu uzyskania dostępu do usługi lub korzystania z niej. Jeżeli małoletni są narażeni na jakiegokolwiek inne zakupy w aplikacji lub w grze, zakupy takie powinny być zawsze wyceniane w walucie krajowej.

- k. Zapewnić, aby małoletni nie byli narażeni na praktyki, które mogą prowadzić do nadmiernych lub niepożądanych wydatków lub nadmiernego korzystania z platformy bądź zachowań kompulsywnych lub nałogowych, poprzez zagwarantowanie, że małoletni nie będą mieć styczności z wirtualnymi przedmiotami, takimi jak płatne skrzynki z łupami, z innymi produktami, w przypadku których oferowane są losowe lub nieprzewidywalne wyniki lub elementy o charakterze zbliżonym do hazardu, oraz poprzez wprowadzenie elementów oddzielających lub spowalniających między treścią a zakupem powiązanych produktów.
- l. Zapewnić, aby małoletni nie byli narażeni na manipulacyjne techniki projektowe ⁽⁸²⁾, takie jak niedobór ⁽⁸³⁾, przyznawane okresowo lub losowo nagrody bądź perswazyjne techniki projektowe ⁽⁸⁴⁾, które mogą prowadzić do nadmiernych, impulsywnych lub niepożądanych wydatków lub zachowań nałogowych.
- m. Zapewnić, aby małoletni nie byli narażeni na niepożądane zakupy, np. poprzez rozważenie wdrożenia skutecznych narzędzi dla opiekunów lub objęcie wszelkich zobowiązań finansowych podjętych przez małoletnich poniżej określonego wieku wymogiem przeglądu lub zgody ze strony opiekunów (zob. sekcja 7.3 dotycząca narzędzi dla opiekunów).

⁽⁸²⁾ Zgodnie z art. 25 rozporządzenia (UE) 2022/2065. Komisja przypomina, że zgodnie z art. 25 ust. 2 zakaz ustanowiony w art. 25 ust. 1 nie ma zastosowania do praktyk objętych dyrektywą 2005/29/WE ani rozporządzeniem (UE) 2016/679.

⁽⁸³⁾ Komisja przypomina, że w załączniku I pkt 7 dyrektywy 2005/29/WE zakazuje się fałszywych twierdzeń, że produkt będzie dostępny jedynie przez ograniczony czas lub że będzie on dostępny na określonych warunkach przez bardzo ograniczony czas, w celu nakłonienia konsumentów do podjęcia natychmiastowej decyzji i pozbawienia ich możliwości świadomego wyboru lub czasu potrzebnego do jego dokonania. W związku z tym przedsiębiorcy podlegają zakazowi stosowania technik niedoboru.

⁽⁸⁴⁾ Komisja przypomina, że w przypadku gier zgodnie z art. 8 i 9 dyrektywy 2005/29/WE przedsiębiorcy nie powinni wykorzystywać błędów behawioralnych ani wprowadzać elementów manipulacyjnych związanych np. z czasem udostępniania ofert w grach (oferowanie mikrotransakcji w krytycznych momentach gry) oraz użyciem efektów wizualnych i akustycznych do wywierania nadmiernej presji na gracza.

- n. Dokonywać przeglądu polityki platformy dotyczącej oferowania transakcji gospodarczych, z uwzględnieniem zmieniających się zdolności dzieci, mając na uwadze, że niektóre grupy wiekowe nie powinny być narażone na transakcje gospodarcze ani nie powinny mieć możliwości zawierania takich transakcji, ponieważ nie są jeszcze w stanie zrozumieć istoty wydatków i pieniędzy.

6.7 Moderacja

70. Moderacja może ograniczyć narażenie małoletnich na treści i zachowania, które są szkodliwe dla ich prywatności, bezpieczeństwa i ochrony, w tym na treści nielegalne lub treści, które mogą zaszkodzić ich rozwojowi fizycznemu lub psychicznemu, a także może przyczynić się do zapobiegania przestępczości.
71. Komisja przypomina o obowiązkach związanych z: warunkami określonymi w art. 14 rozporządzenia (UE) 2022/2065; sprawozdawczością w zakresie przejrzystości, o których mowa w art. 15 wspomnianego rozporządzenia, w odniesieniu do dostawców usług pośrednich, w tym dostawców platform internetowych; mechanizmami zgłaszania i działania oraz uzasadnieniami przewidzianymi, odpowiednio, w art. 16 i 17 wspomnianego rozporządzenia w odniesieniu do dostawców usług hostingu, w tym platform internetowych; zobowiązaniami dostawców platform internetowych dotyczącymi zaufanych podmiotów sygnalizujących ⁽⁸⁵⁾, określonymi w art. 22 wspomnianego rozporządzenia. Przypomina również o kodeksie postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie z 2025 r. oraz o kodeksie postępowania w zakresie zwalczania dezinformacji, które stanowią kodeksy postępowania w rozumieniu art. 45 rozporządzenia (UE) 2022/2065.
72. Komisja uważa, że oprócz wywiązywania się z tych obowiązków dostawcy platform internetowych dostępnych dla małoletnich powinni wprowadzić następujące środki

⁽⁸⁵⁾ Zaufane podmioty sygnalizujące to podmioty dysponujące szczególną wiedzą ekspercką i kompetencjami w zakresie wykrywania niektórych rodzajów nielegalnych treści, a zgłoszenia, których dokonują w wyznaczonych dziedzinach, w których dysponują wiedzą ekspercką, muszą być traktowane priorytetowo i rozpatrywane przez dostawców platform internetowych bez zbędnej zwłoki. Status zaufanego podmiotu sygnalizującego przyznaje koordynator ds. usług cyfrowych państwa członkowskiego, w którym podmiot ma siedzibę, pod warunkiem że podmiot ten wykazał swoją wiedzę ekspercką, kompetencje, niezależność od platform internetowych, a także staranność, dokładność i obiektywizm przy dokonywaniu zgłoszeń.

w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług do celów art. 28 ust. 1 rozporządzenia (UE) 2022/2065, uwzględniając przy tym przede wszystkim najlepszy interes dziecka:

- a. Jasno i przejrzysto określić, co platforma uważa za treści i zachowania szkodliwe dla prywatności, bezpieczeństwa i ochrony małoletnich, we współpracy z małoletnimi, społeczeństwem obywatelskim i niezależnymi ekspertami, w tym środowiskiem akademickim. Powinny one obejmować wszelkie treści i zachowania, które są nielegalne na mocy prawa unijnego lub krajowego. Dostawcy platform internetowych dostępnych dla małoletnich powinni wyraźnie informować małoletnich korzystających ze świadczonych przez nich usług o swoich normach i oczekiwaniach dotyczących treści i zachowań, a informacje te powinny być dostępne podczas tworzenia konta i łatwe do znalezienia na platformie.
- b. Ustanowić zasady i procedury moderacji określające sposoby wykrywania treści i zachowań szkodliwych dla prywatności, bezpieczeństwa i ochrony małoletnich oraz sposoby moderowania takich zachowań w celu ograniczenia narażenia małoletnich na szkodliwe treści. Dostawcy platform internetowych powinni również zapewnić, aby te zasady lub procedury egzekwowano w praktyce.
- c. Poddawać zasady i procedury ocenie i przeglądowi w celu zapewnienia ich skuteczności w miarę zmian technologicznych i zachowań w internecie. W szczególności Komisja uważa, że przy ustalaniu priorytetów w zakresie moderacji dostawcy platform internetowych dostępnych dla małoletnich powinni uwzględniać następujące czynniki: prawdopodobieństwo i dotkliwość powodowanych przez treści szkód dla prywatności, bezpieczeństwa lub ochrony małoletnich, wpływ szkód na małoletnich, szczególne podatności na zagrożenia oraz liczbę małoletnich, którzy mogą doznać szkody. Ponadto priorytetowo należy traktować zgłoszenia dokonywane przez małoletnich.
- d. Oprócz zautomatyzowanego przeglądu treści i wszelkich innych odpowiednich narzędzi, zapewnić dostępność weryfikacji przez człowieka w odniesieniu do zgłaszanych kont lub treści, co do których dostawca podejrzewa, że mogą

stwarzać ryzyko naruszenia prywatności, bezpieczeństwa lub ochrony małoletnich.

- e. Zapewnić, aby zespoły ds. moderowania treści były dobrze przeszkolone i dysponowały odpowiednimi zasobami oraz aby mechanizmy moderacji były zawsze aktywne i funkcjonowały przez cały czas (24 godziny na dobę, 7 dni w tygodniu) w celu zapewnienia skutecznego moderowania, w tym aby przez cały czas co najmniej jeden pracownik pełnił dyżur w celu reagowania na pilne zgłoszenia i sytuacje nadzwyczajne.
- f. Zapewnić dostępność i funkcjonowanie systemów i praktyk moderowania treści w językach urzędowych państwa członkowskiego, w którym świadczona jest usługa.
- g. Wprowadzić skuteczne technologie, mechanizmy wewnętrzne i środki zapobiegawcze w celu zmniejszenia ryzyka, że małoletnim rekomendowane będą treści i zachowania szkodliwe dla ich prywatności, bezpieczeństwa lub ochrony, w tym poprzez wdrożenie skutecznych rozwiązań technicznych, takich jak „hash matching” (dopasowywanie skrótów) i wykrywanie adresów URL, w celu zwalczania znanych szkodliwych i nielegalnych treści. Dostawcy powinni również przeanalizować potencjalne dodatkowe korzyści oferowane przez nowe rozwiązania techniczne, takie jak klasyfikatory sztucznej inteligencji, pod względem wykrywania nowych lub zmienionych treści i zachowań.
- h. Wdrożyć rozwiązania techniczne zapobiegające sytuacjom, w których systemy AI na platformie umożliwiają użytkownikom dostęp do treści szkodliwych dla prywatności, bezpieczeństwa lub ochrony małoletnich, a także dają użytkownikom możliwość generowania i rozpowszechniania takich treści.
- i. Wbudować we wszelkie systemy AI zabezpieczenia, które wykrywają i blokują prompty wskazane przez dostawcę w zasadach moderacji jako szkodliwe dla prywatności, bezpieczeństwa lub ochrony małoletnich. Może

to obejmować na przykład wykorzystanie klasyfikatorów promptów, moderowania treści i innych filtrów ⁽⁸⁶⁾.

- ii. Współpracować z innymi dostawcami platform internetowych i odpowiednimi zainteresowanymi stronami w celu wykrywania naruszających politykę i nielegalnych treści i zachowań oraz zapobiegania rozpowszechnianiu takich treści między platformami.
 - iii. W przypadku gdy dostawca platformy internetowej dostępnej dla małoletnich obsługuje transakcje finansowe, powinien zapewnić specjalny kanał do celów zgłaszania oszustw i podejrzanych transakcji finansowych.
73. Dostawcy platform internetowych dostępnych dla małoletnich powinni udostępniać wskaźniki dotyczące moderowania treści, np. jak często otrzymują zgłoszenia użytkowników, jak często aktywnie wykrywają naruszenia w zakresie treści i zachowania, jakie rodzaje treści i zachowań są zgłaszane i wykrywane oraz jak platforma reagowała na te problemy.
74. Żaden z powyższych środków nie powinien skutkować ogólnym obowiązkiem monitorowania treści, które dostawcy platform internetowych dostępnych dla małoletnich przekazują lub przechowują ⁽⁸⁷⁾.

Złe praktyki

SadShare to platforma społecznościowa, która umożliwia użytkownikom zamieszczanie treści wizualnych i udostępnianie ich innym osobom. Zasady stosowane przez platformę nie obejmują solidnych mechanizmów moderowania treści mających na celu wykrywanie treści szkodliwych i pornograficznych oraz zapobieganie zamieszczaniu takich treści, w tym materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych. Ten brak moderacji naraża zatem małoletnich na nielegalne treści i umożliwia użytkownikom działającym w złej wierze (ponowne) wykorzystywanie istniejących obrazów. To z kolei napędza popyt na materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych, co, w sposób niezamierzony, skłania innych użytkowników do niegodziwego traktowania małoletnich i wyrządzania im szkód w celu tworzenia nowych materiałów.

⁽⁸⁶⁾ Komisja przypomina, że takie użycie systemów sztucznej inteligencji może stanowić zakazaną praktykę w świetle art. 5 ust. 1 lit. b) rozporządzenia (UE) 2024/1689, jeżeli wykorzystują one słabości dzieci w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić poważną szkodę. Wszelkie środki wprowadzane zgodnie z niniejszym zaleceniem powinny wykraczać poza środki wprowadzane w celu uniemożliwienia stosowania tego zakazu. Nadzór nad środkami wprowadzonymi w celu zapewnienia zgodności z art. 50 ust. 1 rozporządzenia (UE) 2024/1689 i egzekwowanie tych środków pozostają w gestii właściwych organów na podstawie wspomnianego rozporządzenia.

⁽⁸⁷⁾ Zob. art. 8 rozporządzenia 2022/2065.

7 ZGŁASZANIE, WSPARCIE UŻYTKOWNIKA I NARZĘDZIA DLA OPIEKUNÓW

7.1 Zgłoszenia użytkowników, informacje zwrotne i skargi

75. Skuteczne, widoczne i przyjazne dziecku narzędzia dokonywania zgłoszeń, przekazywania informacji zwrotnych i składania skarg umożliwiają małoletnim wskazywanie cech platform internetowych, które mogą mieć negatywny wpływ na poziom ich prywatności, bezpieczeństwa i ochrony.
76. Komisja przypomina o obowiązkach ustanowionych w rozporządzeniu (UE) 2022/2065, w tym o obowiązku dotyczącym wprowadzenia mechanizmów zgłaszania i działania (art. 16), przedstawienia uzasadnienia (art. 17), zawiadomienia o podejrzeniu popełnienia przestępstwa (art. 18), wprowadzenia wewnętrznego systemu rozpatrywania skarg (art. 20) oraz pozasądowego rozstrzygania sporów (art. 21), a także o przepisach dotyczących zaufanych podmiotów sygnalizujących (art. 22).
77. Komisja uważa, że oprócz wywiązywania się z tych obowiązków dostawcy platform internetowych dostępnych dla małoletnich powinni wprowadzić następujące środki w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług do celów art. 28 ust. 1 rozporządzenia (UE) 2022/2065:
- a. Wdrożyć mechanizmy zgłaszania, przekazywania informacji zwrotnych i składania skarg, które:
 - i. Są skuteczne, widoczne, przyjazne dziecku i łatwo dostępne (zob. sekcja 6.4 dotycząca projektowania interfejsu internetowego i innych narzędzi oraz sekcja 4 dotycząca zasad ogólnych).
 - ii. Umożliwiają małoletnim zgłaszanie treści, działań, osób, kont lub grup, które ich zdaniem mogą naruszać warunki korzystania z usług platformy. Dotyczy to wszelkich treści, użytkowników czy działań uznanych przez platformę za szkodliwe dla prywatności, bezpieczeństwa lub ochrony małoletnich (zob. sekcja 5 dotycząca przeglądu ryzyka i sekcja 6.7 dotycząca moderacji).

- iii. Umożliwiają wszystkim użytkownikom zgłaszanie treści, działań, osób, kont lub grup, które uznają za nieodpowiednie lub niepożądane dla małoletnich, lub w przypadku gdy wywołuje u nich dyskomfort koncepcja dostępności takich treści, działań, osób fizycznych, kont lub grup dla małoletnich.
- iv. Umożliwiają wszystkim użytkownikom zgłaszanie kont, w przypadku których podejrzewają, że należą do osób poniżej minimalnego wieku, jeżeli w warunkach korzystania z usług platformy określono taki wiek.
- v. Umożliwiają małoletnim przekazywanie informacji zwrotnych na temat wszelkich treści, działań, osób, kont lub grup, które są prezentowane na ich kontach i które wywołują u nich dyskomfort lub które chcą widzieć częściej lub rzadziej. Mogą to być wyrażenia takie jak: „Pokaż mniej/więcej”, „Nie chcę widzieć/nie jestem zainteresowany(-a)”, „Nie chcę widzieć treści z tego konta”, „To powoduje u mnie dyskomfort”, „Ukryj to”, „Nie lubię tego” lub „To nie dla mnie”. Dostawcy platform internetowych powinni zapewnić, aby opcje te były zaprojektowane w sposób gwarantujący ich widoczność tylko dla użytkownika, a co za tym idzie niemożność wykorzystania ich przez inne osoby do szykanowania lub molestowania małoletnich na platformie. Dostawcy platform internetowych powinni dostosowywać systemy rekomendacji w reakcji na takie informacje zwrotne (zob. sekcja 6.5.2 dotycząca kontroli i wzmocnienia pozycji użytkowników) ⁽⁸⁸⁾.
- vi. W przypadku gdy dostawca stosuje metody potwierdzania wieku, mechanizmy te umożliwiają każdemu użytkownikowi dostęp do skutecznego wewnętrznego systemu rozpatrywania skarg, pozwalającego na składanie skarg drogą elektroniczną i nieodpłatnie, na podstawie oceny wieku użytkownika dokonanej przez dostawcę. Taki system rozpatrywania skarg powinien spełniać warunki określone w art. 20 rozporządzenia (UE) 2022/2065.

⁽⁸⁸⁾ Wytyczne dotyczące tego, w jaki sposób takie informacje powinny wpływać na systemy rekomendacji dostawcy, znajdują się w sekcji 6.5.2.

- b. Zapewnić, aby mechanizmy zgłaszania, przekazywania informacji zwrotnych i składania skarg ustanowione na podstawie art. 20 rozporządzenia (UE) 2022/2065 ⁽⁸⁹⁾:
 - i. Przyczyniały się do wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich.
 - ii. Były zgodne z prawami podstawowymi, w szczególności z prawami dziecka.
 - iii. Wszyscy małoletni, w tym osoby z niepełnosprawnościami lub dodatkowymi potrzebami w zakresie dostępności, mogli do nich uzyskać dostęp w sposób intuicyjny i natychmiastowy.
 - iv. Były dla małoletnich łatwe w użyciu i zrozumiałe, dostosowane do wieku i angażujące (zob. sekcja 6.4 dotycząca projektowania interfejsu internetowego i innych narzędzi oraz sekcja 4 dotycząca zasad ogólnych).
 - v. Były dostępne dla niezarejestrowanych użytkowników, jeżeli mają dostęp do treści znajdujących się na platformie internetowej.
- c. Zapewnić dostępność opcji umożliwiającej małoletnim przedstawienie własnego uzasadnienia zgłoszenia lub skargi. Dostawcy powinni unikać stosowania kategorii zgłoszeń, ale jeśli je stosują, powinni zapewnić, aby były one dostosowane do najmłodszych użytkowników dopuszczonych na platformie.
- d. Zapewnić, aby zgłoszenia, informacje zwrotne i skargi były domyślnie poufne i anonimowe, zarazem umożliwiając małoletnim rezygnację z anonimowości. W przypadku rezygnacji z anonimowości dostawca powinien wyjaśnić

⁽⁸⁹⁾ Wszelkie zawarte w pozostałej części niniejszej sekcji odniesienia do „skarg” lub „skargi” obejmują ewentualne skargi dotyczące oceny wieku użytkownika dokonanej przez dostawcę oraz dotyczące decyzji, o których mowa w art. 20 rozporządzenia (UE) 2022/2065. W art. 20 rozporządzenia (UE) 2022/2065 zobowiązano dostawców platform internetowych do zapewnienia odbiorcom usługi dostępu do skutecznego wewnętrznego systemu rozpatrywania skarg w odniesieniu do czterech rodzajów decyzji podjętych przez dostawcę platformy internetowej. Są to: a) decyzje w sprawie usunięcia informacji lub uniemożliwienia do nich dostępu lub ograniczenia widoczności informacji; b) decyzje w sprawie zawieszenia lub zakończenia świadczenia usługi, w pełni lub częściowo, na rzecz odbiorców; c) decyzje w sprawie zawieszenia lub zamknięcia konta odbiorców; oraz d) decyzje w sprawie zawieszenia, zakończenia lub ograniczenia w inny sposób możliwości monetyzacji informacji przekazanych przez odbiorców.

małoletnim, kiedy, w jaki sposób i jakie informacje związane ze zgłoszeniami lub skargami udostępniają innym użytkownikom lub osobom trzecim.

- e. Priorytetowo traktować zgłoszenia dotyczące prywatności, bezpieczeństwa i ochrony małoletnich. Dostawcy platform internetowych powinni zapewnić małoletnim możliwość wskazania, czy uważają zgłoszenie lub skargę za pilne, zwłaszcza gdy istnieją przesłanki wskazujące na występowanie problemu związanego z prywatnością, bezpieczeństwem lub ochroną. Czas reakcji powinien być odpowiedni do problemu będącego przedmiotem zgłoszenia lub skargi. Nie powinno to mieć negatywnego wpływu na priorytetowe traktowanie zgłoszeń dokonywanych przez zaufane podmioty sygnalizujące, zgodnie z art. 22 ust. 1 rozporządzenia (UE) 2022/2065.
- f. Bez zbędnej zwłoki przekazywać potwierdzenie odbioru każdemu małoletniemu, który przekazuje zgłoszenie lub skargę. Małoletnim należy również zapewnić odpowiednie do wieku wyjaśnienie procedury rozpatrywania zgłoszenia lub skargi, a także wyjaśnienie ewentualnie podjętych działań lub ich braku. Informacje te powinny obejmować orientacyjny termin podjęcia decyzji w sprawie zgłoszenia lub skargi oraz możliwych wyników. Komisja jest również zdania, że dostawcy platform internetowych powinni zapewnić mechanizm śledzenia postępów i komunikacji z platformami.
- g. Regularnie dokonywać przeglądu otrzymywanych zgłoszeń, informacji zwrotnych i skarg. Powinni wykorzystywać te informacje do identyfikacji i uwzględnienia wszelkich aspektów swojej platformy, które mogą zagrażać prywatności, bezpieczeństwu lub ochronie małoletnich, doskonalić swoje systemy rekomendacji i praktyki moderacji, poprawiać ogólne normy bezpieczeństwa oraz wspierać bardziej godne zaufania i nacechowane odpowiedzialnością środowisko internetowe. Działania te powinny być udokumentowane, aby można je było poddać przeglądowi.

Złe praktyki

SadLearn to popularna platforma internetowa zaprojektowana dla użytkowników w wieku 6–18 lat. Oferuje różne treści edukacyjne i rozrywkowe. Aby oznaczyć treści niezgodne z warunkami korzystania z usług SadLearn, użytkownik musi kliknąć cztery różne linki. Po dotarciu do sekcji

dotyczącej skarg użytkownik musi dokonać wyboru spośród 15 różnych kategorii skarg, co utrudnia małoletnim zidentyfikowanie i wybranie odpowiedniej kategorii. Nie ma kategorii umożliwiającej wpisanie dowolnego tekstu. Jeżeli użytkownicy zdołają złożyć skargę, nie otrzymują żadnego potwierdzenia ani wyjaśnienia, co stanie się w dalszej kolejności. Ponadto narzędzie zgłaszania jest dostępne wyłącznie w języku angielskim, a użyte sformułowania są dostosowane do odbiorcy dorosłego.

7.2 Środki wsparcia użytkownika

78. Wprowadzenie na platformach internetowych dostępnych dla małoletnich elementów mających pomóc małoletnim w korzystaniu z usług i w razie potrzeby poszukiwaniu wsparcia to skuteczny sposób zapewnienia małoletnim wysokiego poziomu prywatności, bezpieczeństwa i ochrony. Komisja uważa zatem, że dostawcy platform internetowych dostępnych dla małoletnich powinni:
- Udostępniać wyraźnie oznaczone, łatwe do zidentyfikowania i dostępne narzędzia wsparcia, które umożliwiają małoletnim znalezienie pomocy w przypadku napotkania podejrzanych, nielegalnych lub nieodpowiednich treści, kont lub zachowań, które wywołują u nich dyskomfort. Obejmuje to udostępnienie przycisków blokowania i wyciszenia. Narzędzia wsparcia powinny być przyjazne dziecku, wyraźnie widoczne, natychmiastowo dostępne (zob. sekcja 6.4 dotycząca interfejsu internetowego i innych narzędzi) oraz powinny bezpośrednio łączyć małoletnich z usługami wsparcia najodpowiedniejszymi ze względu na ich lokalizację i wiek, takimi jak usługi świadczone przez krajowe centra bezpieczniejszego internetu, stowarzyszenia INHOPE i krajowe telefony zaufania dla dzieci.
 - Ograniczyć stosowanie narzędzi wsparcia opartych na AI, ponieważ nie powinny one być wykorzystywane jako główny mechanizm interakcji z dziećmi.
 - Wprowadzić bezpośrednio widoczne komunikaty ostrzegawcze oraz linki do odpowiednich krajowych infolinii ⁽⁹⁰⁾ i innych autorytatywnych źródeł wyświetlane, gdy małoletni wyszukują, zamieszczają, generują, udostępniają i otrzymują treści potencjalnie nielegalne lub szkodliwe dla ich prywatności, bezpieczeństwa i ochrony (jak wyjaśniono w sekcji 6.7 dotyczącej moderacji).

⁽⁹⁰⁾ Np. należących do krajowych centrów bezpieczniejszego internetu i stowarzyszeń INHOPE lub innych krajowych infolinii dla dzieci, takich jak <https://childhelplineinternational.org/>.

Dostawcy platform internetowych powinni również kierować małoletnich do odpowiednich krajowych infolinii, gdy dokonują oni zgłoszeń dotyczących takich treści. Dostawca platformy internetowej powinien udzielić małoletniemu odpowiednich wskazówek natychmiast po otrzymaniu informacji o takich działaniach lub po dokonaniu zgłoszenia przez małoletniego.

- d. Jeżeli platforma internetowa obejmuje elementy lub funkcje związane z połączeniem użytkownika, zamieszczaniem treści lub komunikacją z użytkownikiem, powinna zapewniać małoletnim możliwość anonimowego blokowania lub wyciszania wszelkich innych użytkowników lub kont, w tym tych, które nie są z nimi powiązane. Systemy blokowania powinny być łatwe do znalezienia i dostępne. Żadne informacje o użytkowniku ani jego koncie nie powinny być dostępne dla kont, które zablokował.
- e. Jeżeli platforma internetowa umożliwia zamieszczanie komentarzy na temat treści, powinna zapewnić małoletnim możliwość ograniczenia rodzajów użytkowników, którzy mogą komentować ich treści i treści ich dotyczące lub uniemożliwić innym użytkownikom komentowanie ich treści i treści ich dotyczących, zarówno w momencie ich zamieszczania, jak i później, nawet jeżeli możliwość komentowania jest ograniczona do kont uprzednio zaakceptowanych przez małoletniego jako kontakty (zgodnie z zaleceniem zawartym w sekcji 6.3 dotyczącej ustawień konta).
- f. Jeżeli platforma internetowa oferuje funkcje grupowe, powinna zapewnić, aby małoletni przystępowali do grup dopiero po otrzymaniu powiadomienia o zaproszeniu i potwierdzeniu, że chcą należeć do danej grupy.

Dobre praktyki

NiceSpace to platforma społecznościowa dla użytkowników w wieku powyżej 13 lat. Podczas rejestracji użytkownicy zapoznają się z interaktywnym instruktażem „SafeSpace 101”, w ramach którego otrzymują wyjaśnienia dotyczące elementów platformy zapewniających prywatność, bezpieczeństwo i ochronę, w tym opcji blokowania i wyciszania, kontroli komentarzy i zaproszeń do grup. NiceSpace posiada również dobrze widoczny przycisk „Pomoc”, łączący użytkowników bezpośrednio z infolinią lokalnego centrum bezpieczniejszego internetu. Podczas wyszukiwania potencjalnie szkodliwych treści NiceSpace ostrzega użytkowników za pomocą podpowiedzi kontekstowych

7.3 Narzędzia dla opiekunów

79. 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.
80. Komisja uważa, że narzędzia dla opiekunów należy traktować jako uzupełnienie środków z zakresu bezpieczeństwa już w fazie projektowania i domyślnego bezpieczeństwa oraz wszelkich innych środków wprowadzonych w celu zapewnienia zgodności z art. 28 ust. 1 rozporządzenia (UE) 2022/2065, w tym środków opisanych w niniejszych wytycznych. Przestrzeganie przez dostawców platform internetowych dostępnych dla małoletnich obowiązku zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony w ramach świadczonych przez siebie usług nie może nigdy opierać się wyłącznie na narzędziach dla opiekunów. Narzędzia dla opiekunów nie powinny służyć wyłącznie do zapewniania wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich na platformach internetowych ani do *zastępowania* jakichkolwiek innych środków wprowadzanych w tym celu. Środki takie mogą nie odzwierciedlać realiów życia dzieci, w szczególności w przypadku podzielonej pieczy nad dzieckiem, rodzinnej pieczy zastępczej lub gdy opiekunowie są nieobecni lub nie angażują się w opiekę. Ponadto skuteczność zgody rodziców jest ograniczona w przypadku gdy nie weryfikuje się w sposób wiarygodny tożsamości lub władzy rodzicielskiej osoby dorosłej wyrażającej zgodę. Dostawcy platform internetowych dostępnych dla małoletnich muszą zatem wdrażać odpowiednie środki ochrony małoletnich i nie należy ich ograniczać do oparcia się na nadzorze rodzicielskim. Komisja zauważa jednak, że narzędzia dla opiekunów, stosowane w połączeniu z innymi środkami, mogą przyczynić się do osiągnięcia tak wysokiego poziomu.
81. W związku z tym Komisja uważa, że dostawcy platform internetowych dostępnych dla małoletnich powinni wprowadzić narzędzia kontroli dla opiekunów do celów art. 28 ust. 1 rozporządzenia (UE) 2022/2065, które powinny:

- a. Być dostosowane do wieku i do zmieniających się zdolności małoletnich. Narzędzia dla opiekunów powinny opierać się na komunikacji, uczeniu się i upodmiotowieniu, a nie na kontroli, i zapewniać małoletnim autonomię i sprawczość. Powinny one być skuteczne i nie powinny w nieproporcjonalny sposób ograniczać praw małoletnich do prywatności lub dostępu do usług, przy czym należy przede wszystkim uwzględniać najlepszy interes małoletniego.
 - b. Być łatwe w użyciu, dostępne i aktywacji, na przykład umożliwiając opiekunowi korzystanie z narzędzia bez tworzenia konta w ramach usługi.
 - c. Mieć zastosowanie niezależnie od urządzenia czy systemu operacyjnego wykorzystywanego do uzyskania dostępu do usługi.
 - d. Przekazywać małoletnim jasne powiadomienia o aktywacji przez opiekunów i obejmować inne zabezpieczenia, uwzględniające potencjalne niewłaściwe wykorzystanie przez opiekunów, takie jak na przykład wyraźne sygnalizowanie małoletniemu w czasie rzeczywistym, gdy aktywowana jest jakakolwiek funkcja monitorowania.
 - e. Zapewniać, aby zmiany można było wprowadzać wyłącznie przy takim samym stopniu upoważnienia, jaki wymagany jest przy pierwszej aktywacji narzędzi.
 - f. Być kompatybilne z dostępnością interoperacyjnych rozwiązań kompleksowej obsługi dla opiekunów, obejmujących wszystkie ustawienia i narzędzia.
82. Narzędzia dla opiekunów mogą obejmować funkcje zarządzania ustawieniami domyślnymi, ustawienia ograniczeń czasu spędzanego przed ekranem (zob. sekcja 6.4 dotycząca projektu interfejsu internetowego i innych narzędzi), przeglądania kont, z którymi komunikuje się małoletni, zarządzania ustawieniami konta, ustalania, w stosownych przypadkach, domyślnych limitów wydatków dla małoletniego lub inne funkcje służące nadzorowaniu korzystania z platform internetowych, które mogą być szkodliwe dla prywatności, bezpieczeństwa i ochrony małoletniego.

8 ZARZĄDZANIE

83. Dobre zarządzanie platformami to skuteczny sposób zapewniania, aby ochrona małoletnich była należycie traktowana priorytetowo i zarządzana na całej platformie,

co przyczynia się do zapewnienia wymaganego wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich.

8.1 Zarządzanie (ogólne)

84. Komisja uważa, że dostawcy platform internetowych dostępnych dla małoletnich powinni wprowadzić skuteczne praktyki zarządzania w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług do celów art. 28 ust. 1 rozporządzenia (UE) 2022/2065. Obejmuje to między innymi:

- a. Wdrażanie zasad wewnętrznych określających, w jaki sposób dostawca platformy internetowej ma zapewniać wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich korzystających ze świadczonych przez niego usług.
- b. Powierzenie specjalnie wyznaczonej osobie lub zespołowi odpowiedzialności za zapewnienie wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich. Ta osoba lub zespół powinni dysponować wystarczającymi zasobami, a także wystarczającymi uprawnieniami, aby mieć bezpośredni dostęp do kadry kierowniczej wyższego szczebla dostawcy platformy internetowej, a także powinni być centralnym punktem kontaktowym dla organów regulacyjnych, użytkowników i zaufanych podmiotów sygnalizujących w sprawach związanych z prywatnością, bezpieczeństwem i ochroną małoletnich.
- c. Propagowanie kultury prywatności, bezpieczeństwa i ochrony małoletnich korzystających z usługi. Obejmuje to:
 - i. Propagowanie i priorytetowe traktowanie kultury uczestnictwa dzieci w projektowaniu i funkcjonowaniu platformy. Cele te należy realizować w sposób bezpieczny, etyczny, inkluzywny i znaczący, w najlepszym interesie dzieci, a także zapewnić mechanizmy przekazywania informacji

zwrotnych, aby wyjaśniać małoletnim, w jaki sposób uwzględniono ich poglądy ⁽⁹¹⁾.

- ii. Zwiększanie świadomości tego, jak dostawca usług przestrzega praw dziecka na swojej platformie, oraz na temat zagrożeń, na jakie mogą być narażeni małoletni na platformie pod względem prywatności, bezpieczeństwa lub ochrony ⁽⁹²⁾.
- iii. Zapewnienie odpowiednich szkoleń i informacji osobom odpowiedzialnym za prywatność, bezpieczeństwo i ochronę małoletnich, programistom, osobom odpowiedzialnym za moderację lub osobom przyjmującym zgłoszenia lub skargi od małoletnich ⁽⁹³⁾.
- iv. Posiadanie procedur zapewniających regularne monitorowanie zgodności z art. 28 ust. 1 rozporządzenia (UE) 2022/2065.
- v. Zapewnienie, aby wszelkie rozwiązania technologiczne i organizacyjne stosowane w celu wdrożenia niniejszych wytycznych były zgodne z aktualnym stanem wiedzy i z krajowymi wytycznymi dotyczącymi

⁽⁹¹⁾ W wytycznych UNICEF-u dotyczących zaangażowania zainteresowanych stron w sprawy dzieci przedstawiono konkretne kroki w zakresie odpowiedzialnego uczestnictwa dzieci. UNICEF (2025). *Spotlight guidance on best practices for stakeholder engagement with children in D-CRIAs* [Wytyczne dotyczące najlepszych praktyk w zakresie zaangażowania zainteresowanych stron w sprawy dzieci w ramach cyfrowych ocen wpływu na prawa dziecka]. Dostępne na stronie: <https://www.unicef.org/childrightsandbusiness/media/1541/file/D-CRIA-Spotlight-Guidance-Stakeholder-Engagement.pdf>.

⁽⁹²⁾ Podejście to jest zgodne ze strategią na rzecz lepszego internetu dla dzieci (BIK+), w której podkreślono znaczenie świadomości i edukacji dla zwiększania bezpieczeństwa w internecie i która wspiera wdrażanie rozporządzenia (UE) 2022/2065 w tym zakresie. Ponadto centra bezpieczniejszego internetu, utworzone w każdym państwie członkowskim, świadczą o wartości wysiłków na rzecz podnoszenia świadomości w zakresie zapobiegania szkodom i zagrożeniom w internecie oraz reagowania na nie.

⁽⁹³⁾ Szkolenie to może obejmować np. prawa dzieci, zagrożenia i szkody pod względem prywatności, bezpieczeństwa i ochrony małoletnich w internecie, a także skuteczne praktyki w zakresie zapobiegania, reagowania i zmniejszania ryzyka.

ochrony małoletnich ⁽⁹⁴⁾, prawami dziecka i najwyższymi dostępnymi standardami ⁽⁹⁵⁾.

- vi. Wprowadzenie procesu regularnego gromadzenia i rejestrowania na platformie danych dotyczących szkód i zagrożeń związanych z prywatnością, bezpieczeństwem i ochroną małoletnich, które to dane należy okresowo przedstawiać kierownictwu dostawcy, a także osobie lub zespołowi wyznaczonemu do ochrony małoletnich. Pozostaje to bez uszczerbku dla obowiązków dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych wynikających z art. 34 i 35 rozporządzenia (UE) 2022/2065.
- vii. Prowadzenie między platformami a dostawcami, a także z koordynatorami ds. usług cyfrowych, zaufanymi podmiotami sygnalizującymi, organizacjami społeczeństwa obywatelskiego, środowiskiem akademickim i innymi odpowiednimi zainteresowanymi stronami, wymiany dobrych praktyk i rozwiązań technologicznych, które mają na celu zapewnienie wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich. Współpraca między platformami powinna obejmować wykrywanie ryzyka, normy projektowania i współpracę badawczą z zaufanymi podmiotami.

⁽⁹⁴⁾ An Coimisiún um Chosaint Sonraí (2021). *Fundamentals for a child-oriented approach to data processing* [Podstawy ukierunkowanego na dzieci podejścia do przetwarzania danych]. Dostępne na stronie: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf; Coimisiún na Meán (2024). *Online safety code* [Kodeks bezpieczeństwa w internecie]. Dostępne na stronie: <https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf>; IMY (Szwedzki Urząd Ochrony Danych) (2021). *The rights of children and young people on digital platforms* [Prawa dzieci i młodzieży na platformach cyfrowych]. Dostępne na stronie: <https://www.imy.se/en/publications/the-rights-of-children-and-young-people-on-digital-platforms/>; Nederlandse Ministerie van Justitie (2022). *Code for children's rights* [Kodeks praw dziecka]. Dostępne na stronie: <https://codevoorkinderrechten.waag.org/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf>; CNIL (2021). *CNIL publishes 8 recommendations to enhance protection of children online* [CNIL publikuje osiem zaleceń dotyczących poprawy ochrony dzieci w internecie]. Dostępne na stronie: <https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online>; Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs (brak daty). *Rechtsfragen Digitales*. Dostępne na stronie: <https://beauftragte-missbrauch.de/themen/recht/rechtsfragen-digitales>.

⁽⁹⁵⁾ CEN-CENELEC (2023) *Workshop Agreement 18016 Age Appropriate Digital Services Framework* [Porozumienie robocze 18016 Odpowiednie do wieku ramy usług cyfrowych]; OECD (2021). *Children in the digital environment - Revised typology of risks* [Dzieci w środowisku cyfrowym – zmieniona typologia ryzyka]. https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html.

8.2 Warunki korzystania z usług

85. Warunki korzystania z usług zapewniają ramy regulujące stosunki między dostawcą platformy internetowej a jej użytkownikami. Określają one zasady i oczekiwania dotyczące zachowań w internecie oraz odgrywają ważną rolę w tworzeniu bezpiecznego i zapewniającego poszanowanie prywatności środowiska ⁽⁹⁶⁾.
86. Komisja przypomina o obowiązkach spoczywających na wszystkich dostawcach usług pośrednich w odniesieniu do warunków korzystania z usług określonych w art. 14 rozporządzenia (UE) 2022/2065, w tym o obowiązku wyjaśnienia przez dostawców usług pośrednich warunków i ograniczeń korzystania z usługi w jasnym, prostym, zrozumiałym, przyjaznym dla użytkownika i jednoznacznym języku. Ponadto art. 14 ust. 3 wspomnianego rozporządzenia stanowi, że jeżeli usługa pośrednia jest skierowana przede wszystkim do małoletnich lub gdy korzystają z niej w głównej mierze małoletni, należy zapewnić te informacje w sposób zrozumiały dla małoletnich ⁽⁹⁷⁾ ⁽⁹⁸⁾.
87. Ponadto Komisja uważa, że dostawcy platform internetowych dostępnych dla małoletnich powinni zapewnić, aby warunki świadczonej przez nich usługi:
- a. Obejmowały informacje na temat:
 - i. Kroków, które muszą wykonać użytkownicy, od momentu utworzenia konta do jego usunięcia.
 - ii. Wytycznych dla społeczności służących budowaniu pozytywnej, bezpiecznej i inkluzywnej atmosfery oraz wyjaśniających, jakiego rodzaju

⁽⁹⁶⁾ W normie P2089.2TM dotyczącej warunków korzystania przez dzieci z internetu określono procesy i praktyki służące opracowaniu warunków korzystania z usług, które pomagają chronić prawa dzieci w środowisku cyfrowym.

⁽⁹⁷⁾ Komisja przypomina również, że zgodnie z art. 28b dyrektywy 2010/13/UE na dostawcach platform udostępniania wideo spoczywają wymogi dotyczące ochrony małoletnich przed audycjami, filmami wideo stworzonymi przez użytkowników i handlowymi przekazami audiowizualnymi, które mogą szkodzić ich rozwojowi fizycznemu, psychicznemu lub moralnemu. Stosowanie tych wymogów ma zostać ocenione i ewentualnie poddane przeglądowi do dnia 19 grudnia 2026 r.

⁽⁹⁸⁾ Jak wskazano we wprowadzeniu do niniejszych wytycznych, niektóre przepisy rozporządzenia (UE) 2022/2065, w tym art. 14 pkt 5 i 6, nakładają dodatkowe obowiązki na dostawców bardzo dużych platform internetowych. W zakresie, w jakim obowiązki określone w tych przepisach odnoszą się również do prywatności, bezpieczeństwa i ochrony małoletnich w rozumieniu art. 28 ust. 1, niniejsze wytyczne opierają się na tych przepisach.

zachowania są oczekiwane i zakazane w ramach świadczonej przez usługi oraz jakie są konsekwencje nieprzestrzegania zasad.

- iii. Rodzajów treści i zachowań, które uznaje się za szkodliwe dla prywatności, bezpieczeństwa lub ochrony małoletnich. Dotyczy to m.in. nielegalnych treści, które są szkodliwe dla prywatności, bezpieczeństwa lub ochrony małoletnich, oraz rozpowszechniania tych treści.
 - iv. Tego, w jaki sposób małoletni są chronieni przed takimi treściami i zachowaniami.
 - v. Narzędzi wykorzystywanych do zapobiegania, łagodzenia i moderacji w odniesieniu do treści, zachowań i funkcji, które są nielegalne lub szkodliwe dla prywatności, bezpieczeństwa i ochrony małoletnich, a także procesu rozpatrywania skarg.
- b. Były łatwe do znalezienia i przeszukiwania przez cały czas korzystania z platformy przez użytkownika.
 - c. Nie ograniczały nadmiernie żadnych praw małoletnich, w tym ich prawa do wolności wypowiedzi i informacji.
 - d. Były stosowane i wdrażane w praktyce.
88. Ponadto Komisja uważa, że dostawcy platform internetowych dostępnych dla małoletnich powinni zapewnić rejestrowanie i publikowanie zmian w warunkach korzystania z usług ⁽⁹⁹⁾.

Dobre praktyki

HappyExplore to platforma internetowa, na której małoletni mogą grać w gry oraz tworzyć i odkrywać stworzenia i światy, które mogą sobie wzajemnie udostępniać. Na HappyExplore funkcjonuje postać znana jako „Pixel Pioneer”, która uczy użytkowników, jak być odpowiedzialnymi odkrywcami. Wszystkich użytkowników zachęca się, aby podjęli „zobowiązanie do uprzejmości”, w ramach którego uczą się uprzejmego i bezpiecznego zachowania w internecie i obiecują stosować się do jego zasad. Pixel Pioneer wyjaśnia również, jak ważna jest moderacja i podejmowanie decyzji dotyczących bezpieczeństwa dla użytkowników, którzy odkrywają platformę, np. dlaczego powinni dobrze zastanowić się, zanim udostępnią swoje stworzenia lub światy.

⁽⁹⁹⁾ Np. poprzez opublikowanie ich w bazie danych warunków korzystania z usług cyfrowych: <https://platform-contracts.digital-strategy.ec.europa.eu/>

8.3 Monitorowanie i ocena

89. Komisja uważa, że dostawcy platform internetowych dostępnych dla małoletnich powinni przyjąć skuteczne praktyki monitorowania i oceny w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług do celów art. 28 ust. 1 rozporządzenia (UE) 2022/2065. Obejmuje to między innymi:

- a. Regularne monitorowanie i ocenę skuteczności wszelkich elementów platformy, które dotyczą prywatności, bezpieczeństwa i ochrony małoletnich na platformie. Dotyczy to np. interfejsu internetowego platformy, systemów, ustawień, narzędzi, funkcji i cech oraz mechanizmów dokonywania zgłoszeń, przekazywania informacji zwrotnych i składania skarg, a także środków wprowadzonych w celu zapewnienia zgodności z art. 28 ust. 1 rozporządzenia (UE) 2022/2065 ⁽¹⁰⁰⁾. Dostawcy powinni rozważyć udostępnienie tych ocen niezależnym stronom trzecim, takim jak eksperci lub inne odpowiednie zainteresowane strony, które w ten sposób uzyskają wgląd do nich i możliwość wniesienia wkładu.
- b. Regularne konsultacje z małoletnimi, opiekunami, środowiskiem akademickim, organizacjami społeczeństwa obywatelskiego, ekspertami w dziedzinie praw dziecka i innymi odpowiednimi zainteresowanymi stronami w sprawie projektowania i oceny wszelkich elementów platformy, które dotyczą prywatności, bezpieczeństwa i ochrony małoletnich na platformie. Powinny one obejmować testowanie tych elementów z udziałem małoletnich i uwzględnianie przekazywanych przez nich informacji zwrotnych. Aby przyczynić się do niedyskryminacji i dostępności, dostawcy usług powinni, w miarę możliwości, angażować w te konsultacje małoletnich z różnych środowisk kulturowych

⁽¹⁰⁰⁾ Jak wskazano w sekcji dotyczącej zakresu niniejszych wytycznych (sekcja 2), niektóre przepisy rozporządzenia (UE) 2022/2065, w tym rozdział III sekcja 5, nakładają dodatkowe obowiązki na dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. W zakresie, w jakim obowiązki określone w tych przepisach odnoszą się również do prywatności, bezpieczeństwa i ochrony małoletnich w rozumieniu art. 28 ust. 1, niniejsze wytyczne opierają się na tych przepisach, a bardzo duże platformy internetowe nie powinny oczekiwać, że przyjęcie środków opisanych w niniejszych wytycznych, w części lub w całości, wystarczy do wywiązania się z obowiązków, które spoczywają na nich na mocy rozdziału III sekcja 5 rozporządzenia (UE) 2022/2065.

i językowych, w różnym wieku, z niepełnosprawnościami lub dodatkowymi potrzebami w zakresie dostępności.

- c. Dostosowanie projektu i funkcjonowania wyżej wymienionych elementów z uwzględnieniem wyników tych konsultacji oraz rozwoju technicznego, badań, zmian w zachowaniu użytkowników lub polityce, zmian dotyczących produktów i zastosowań oraz zmian w zakresie szkód i zagrożeń dla prywatności, bezpieczeństwa i ochrony małoletnich na platformie.

8.4 Przejrzystość

- 90. Komisja przypomina o obowiązkach w zakresie przejrzystości wynikających z art. 14, 15 i 24 rozporządzenia (UE) 2022/2065. Ze względu etapy rozwoju i zmieniające się zdolności małoletnich, należy rozważyć dodatkowe kwestie dotyczące przejrzystości funkcjonowania platformy internetowej, aby zapewnić zgodność z art. 28 ust. 1 wspomnianego rozporządzenia.
- 91. Komisja uważa, że dostawcy platform internetowych dostępnych dla małoletnich powinni zapewnić, aby wszelkie niezbędne i istotne informacje na temat funkcjonowania ich usług były łatwo dostępne dla małoletnich, co zagwarantuje wysoki poziom prywatności, bezpieczeństwa i ochrony w ramach świadczonych przez nich usług. Uważa, że dostawcy platform internetowych powinni udostępniać małoletnim oraz, w stosownych przypadkach, ich opiekunom, za pośrednictwem dostępnego interfejsu na swoich platformach internetowych, następujące informacje:
 - a. Informacje o wszelkich środkach wprowadzonych w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa lub ochrony małoletnich na platformie. Informacje te dotyczą m.in.:
 - i. wszelkich zastosowanych metod potwierdzania wieku, zasady działania tych metod oraz wszelkich osób trzecich, za pomocą których stosuje się ewentualne metody weryfikacji lub szacowania wieku;
 - ii. funkcjonowania systemów rekomendacji stosowanych na całej platformie oraz poszczególnych opcji dostępnych dla użytkowników (zob. sekcja 6.5.2 dotycząca kontroli i wzmocnienia pozycji użytkowników);

- iii. procesów reagowania na wszelkie zgłoszenia, informacje zwrotne i skargi składane lub przekazywane przez małoletnich, w tym orientacyjnych ram czasowych oraz możliwych wyników i skutków tych procesów;
 - iv. narzędzi, produktów i funkcji AI wykorzystywanych na platformie, ich ograniczeń i potencjalnych konsekwencji ich użycia;
 - v. procesu rejestracji, o ile jest oferowany;
 - vi. wszelkich oferowanych opiekunom narzędzi, z podaniem wyjaśnienia, jak z nich korzystać i w jaki sposób chronią one małoletnich w internecie, a także jakiego rodzaju informacje o aktywności internetowej małoletniego mogą uzyskać za pomocą takich narzędzi opiekunowie;
 - vii. tego, w jaki sposób moderuje się treści naruszające warunki korzystania z usług platformy i jakie są konsekwencje takiej moderacji;
 - viii. tego, jak korzystać z poszczególnych narzędzi dokonywania zgłoszeń, składania skarg, dochodzenia roszczeń i wsparcia, o których mowa w niniejszych wytycznych;
 - ix. warunków korzystania z usług platformy internetowej;
 - x. wszelkich innych środków zalecanych w niniejszych wytycznych i wprowadzonych przez dostawcę platformy internetowej;
 - xi. wszelkich innych przyjętych środków lub zmian wprowadzonych w świadczonych usługach w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa lub ochrony małoletnich na platformie.
- b. Zapewnić, aby informacje te, wszystkie ostrzeżenia i wszelkie inne komunikaty zalecane w niniejszych wytycznych były:
- i. przyjazne dziecku, dostosowane do wieku, łatwe do zrozumienia i łatwo dostępne dla wszystkich małoletnich, w tym osób z niepełnosprawnościami lub dodatkowymi potrzebami w zakresie dostępności;
 - ii. przedstawione w sposób łatwy do zrozumienia oraz możliwie najprostszy i zwięzły. Np. w przypadku gdy warunki korzystania z usług odnoszą się

do konkretnej funkcji, kluczowe informacje na temat tej funkcji przedstawia się w momencie, gdy małoletni z niej korzysta;

- iii. przedstawione małoletniemu w sposób łatwy do zweryfikowania i zapewniający natychmiastowy i intuicyjny dostęp w momentach, w których stają się istotne;
 - iv. przedstawione w językach urzędowych państwa członkowskiego, w którym świadczona jest usługa;
 - v. angażujące dla małoletnich. Może to wymagać wykorzystania grafik, filmów wideo lub postaci bądź innych technik;
 - vi. podawane małoletnim stopniowo z upływem czasu w celu zmaksymalizowania ilości informacji zapamiętanych przez użytkownika.
- c. Wszelkie środki i zmiany wprowadzone w celu zapewnienia zgodności z art. 28 ust. 1 rozporządzenia (UE) 2022/2065 mogą być komunikowane wewnętrznie i w miarę możliwości podawane do wiadomości publicznej.

Dobre praktyki

HappyTerms to platforma internetowa przeznaczona dla osób w wieku od 13 do 18 lat. Oferuje ona małoletnim możliwość uczestniczenia w życiu społeczności oraz wymiany pomysłów i informacji na temat wspólnych zainteresowań. HappyTerms prezentuje informacje na temat warunków korzystania z usług, wyświetlając wyraziste nagłówki, którym towarzyszą ikony wyjaśniające i kolorowe obrazy. Zasady są podzielone na krótkie, łatwe do przeczytania sekcje i wyjaśnione za pomocą prostego języka. Dostępne są również infografiki, które pomagają małoletnim zrozumieć, na co się zgadzają – infografiki wyświetlane są w momentach, gdy stają się istotne w odniesieniu do danej cechy lub zmiany ustawień. Użytkownicy mogą również zapoznać się z zasadami, klikając ikonę „Co muszę wiedzieć”, dzięki której z dowolnej części platformy mogą przejść do odpowiednich zasad, powiązanych narzędzi i przydatnych linków. HappyTerms oferuje również interaktywny quiz, za pomocą którego małoletni mogą sprawdzić, czy zrozumieli warunki korzystania z usług.

9 PRZEGLĄD

92. Komisja dokona przeglądu niniejszych wytycznych, gdy tylko będzie to konieczne, a najpóźniej po upływie 12 miesięcy, uwzględniając praktyczne doświadczenia zdobyte podczas stosowania art. 28 ust. 1 rozporządzenia (UE) 2022/2065 oraz tempo zmian technologicznych, społecznych i regulacyjnych w tym obszarze.

93. Komisja będzie zachęcać dostawców platform internetowych dostępnych dla małoletnich, koordynatorów ds. usług cyfrowych, właściwe organy krajowe, środowisko badawcze i organizacje społeczeństwa obywatelskiego do wnoszenia wkładu w ten proces. Po przeprowadzeniu takiego przeglądu Komisja może, w porozumieniu z Europejską Radą ds. Usług Cyfrowych, podjąć decyzję o zmianie niniejszych wytycznych.

Załącznik

5C – typologia ryzyka dla dzieci w internecie

94. OECD ⁽¹⁰¹⁾ i badacze ⁽¹⁰²⁾ sklasyfikowali rodzaje ryzyka ⁽¹⁰³⁾, jakie mogą napotkać małoletni w internecie, aby dostawcy platform internetowych dostępnych dla małoletnich, środowiska akademickie i decydenci mogli je lepiej zrozumieć i przeanalizować. Tę klasyfikację ryzyka określa się mianem typologii 5C ryzyka dla dzieci w internecie. Pomaga identyfikować ryzyko i obejmuje pięć kategorii tego ryzyka: ryzyko dotyczące treści (content), zachowań (conduct), kontaktu (contact), ryzyko dla konsumentów (consumer risk) i przekrojowe czynniki ryzyka (cross-cutting risks). Te rodzaje ryzyka mogą występować, gdy nie wprowadzono odpowiednich i proporcjonalnych środków zapewniających wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich korzystających ze świadczonej usługi, co może doprowadzić do naruszenia szeregu praw dziecka.

95. 5C – typologia ryzyka dla dzieci w internecie ⁽¹⁰⁴⁾

Ryzyko dla dzieci w środowisku cyfrowym				
Kategorie ryzyka	Treści	Zachowanie	Kontakt	Ryzyko dla konsumentów
Przekrojowe czynniki ryzyka	Dodatkowe ryzyko dla prywatności, bezpieczeństwa i ochrony Ryzyko związane z zaawansowanymi technologiami Ryzyko dla zdrowia i dobrostanu Ryzyko niewłaściwego wykorzystania			
	Nienawistne	Nienawistne	Spotkania	Ryzyko związane

⁽¹⁰¹⁾ OECD (2021). Children in the digital environment - Revised typology of risks [Dzieci w środowisku cyfrowym – zmieniona typologia ryzyka]. https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html.

⁽¹⁰²⁾ Livingstone, S., i Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children* [4C: klasyfikacja ryzyka dla dzieci w internecie] (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>.

⁽¹⁰³⁾ Zob. również analiza ryzyka przedstawiona przez Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) (2022). *Gefährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln. Aktualisierte und erweiterte 2. Auflage.* - Bundeszentrale für Kinder- und Jugendmedienschutz. Dostępne na stronie: <https://www.bzkg.de/resource/blob/197826/5e88ec66e545bcb196b7bf81fc6dd9e3/2-auflage-gefaehrungsatlas-data.pdf>.

⁽¹⁰⁴⁾ OECD (2021). *Children in the digital environment - Revised typology of risks* s. 7 [Dzieci w środowisku cyfrowym – zmieniona typologia ryzyka]. https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html.

Przejawy ryzyka	treści	zachowania	z nienawiścią	z marketingiem
	Szkodliwe treści	Szkodliwe zachowania	Szkodliwe spotkania	Ryzyko związane z profilowaniem handlowym
	Treści niezgodne z prawem	Zachowania niezgodne z prawem	Nielegalne spotkania	Ryzyko finansowe
	Dezinformacja	Problematiczne zachowania generowane przez użytkowników	Inne problematyczne spotkania	Zagrożenia bezpieczeństwa

96. **Ryzyko dotyczące treści:** Małoletni mogą być nieoczekiwanie i nieumyślnie narażeni na treści potencjalnie dla nich szkodliwe: a) nienawistne treści; b) szkodliwe treści; c) nielegalne treści; d) dezinformację. Powszechnie uznaje się, że tego rodzaju treści mają poważne negatywne konsekwencje dla zdrowia psychicznego i dobrostanu fizycznego małoletnich, np. treści propagujące samookaleczenia, samobójstwa, zaburzenia odżywiania lub skrajną przemoc.
97. **Ryzyko dotyczące zachowań:** Odnosi się do zachowań, które małoletni mogą aktywnie wykazywać w internecie i które mogą stanowić zagrożenie zarówno dla nich, jak i dla innych osób – mogą to być np.: a) nienawistne zachowania (np. małoletni zamieszczający/przesyłający nienawistne treści/wiadomości); b) szkodliwe zachowania (np. małoletni zamieszczający/wysyłający treści przedstawiające przemoc lub treści pornograficzne); c) zachowanie niezgodne z prawem (np. małoletni zamieszczający/wysyłający materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych lub treści o charakterze terrorystycznym); oraz d) problematyczne zachowania generowane przez użytkowników (np. udział w niebezpiecznych wyzwaniach; sexting).
98. **Ryzyko związane z kontaktem:** Odnosi się do sytuacji, w których małoletni są ofiarami interakcji, nie zaś aktywnym podmiotem: a) spotkań z nienawiścią; b) szkodliwych spotkania (np. celem spotkania jest wyrządzenie szkody małoletniemu); c) nielegalnych spotkania (np. mogących podlegać ściganiu na mocy prawa karnego); oraz d) innych problematycznych spotkań. Przykłady ryzyka związanego z kontaktem to m.in. uwodzenie dzieci przez internet, zmuszanie do czynności seksualnych i wymuszenia seksualne wobec dzieci w internecie, niegodziwe traktowanie w celach seksualnych przy wykorzystaniu kamer internetowych, cyberszykanowanie i handel ludźmi do celów wykorzystywania seksualnego. Ryzyko

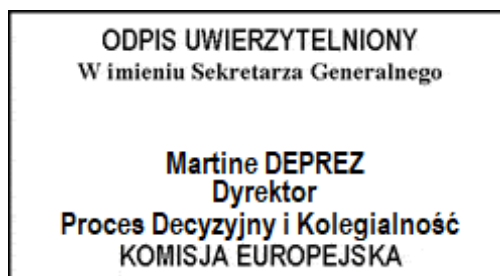
to obejmuje również oszustwa internetowe, takie jak phishing, oszustwa na platformach sprzedażowych i kradzież tożsamości.

99. **Ryzyko dla konsumentów:** Małoletni mogą być również narażeni na ryzyko jako konsumenci w gospodarce cyfrowej: a) ryzyko związane z marketingiem (np. skrzynki z łupami, gry reklamowe); b) ryzyko związane z profilowaniem handlowym (np. lokowanie produktu lub otrzymywanie reklam przeznaczonych dla dorosłych, takich jak reklamy usług randkowych); c) ryzyko finansowe (np. oszustwa lub wydatkowanie dużych kwot pieniędzy bez wiedzy lub zgody opiekunów); d) ryzyko dla bezpieczeństwa i e) ryzyko związane z zakupem i spożywaniem narkotyków, leków, alkoholu i innych nielegalnych lub niebezpiecznych produktów. Ryzyko dla konsumentów obejmuje również ryzyko związane z umowami, np. ze sprzedażą danych użytkowników lub nieuczciwymi warunkami korzystania z usług.
100. **Przekrojowe czynniki ryzyka:** Są to czynniki ryzyka obejmujące wszystkie kategorie ryzyka i uważane za wysoce problematyczne, ponieważ mogą znacząco wpływać na życie małych na wiele sposobów. Są to:
- a. **Ryzyko związane z zaawansowanymi technologiami** – w miarę rozwoju technologii małe napotykają nowe zagrożenia, takie jak chatboty AI, które mogą podawać szkodliwe informacje lub być wykorzystywane do nagabywania dzieci w celach seksualnych poprzez wykorzystywanie luk w zabezpieczeniach, czy też zastosowanie technologii biometrycznych, które może prowadzić do nadużyć, oszustw dotyczących tożsamości i do wykluczenia.
 - b. **Ryzyko dla zdrowia i dobrostanu** – dotyczy potencjalnych szkód dla dobrostanu psychicznego, emocjonalnego lub fizycznego małych. Może to być np. częstsze występowanie otyłości/anoreksji i problemów ze zdrowiem psychicznym związane z korzystaniem z platform internetowych lub nadmiernym korzystaniem z nich, co w niektórych przypadkach może mieć negatywny wpływ na zdrowie fizyczne i psychiczne oraz dobrostan małych, prowadząc do takich problemów, jak uzależnienie, depresja, zaburzenia lękowe, zaburzenia snu i izolacja społeczna.
 - c. **Dodatkowe zagrożenia dotyczące prywatności i ochrony danych** – wynikają z dostępu do informacji na temat małych oraz z niebezpieczeństwa

związanego z funkcjami geolokalizacyjnymi, które przestępcy mogą wykorzystać w celu zlokalizowania małoletnich i zbliżenia się do nich.

101. Inne przekrojowe czynniki ryzyka ⁽¹⁰⁵⁾ mogą również obejmować:

- a. **Dodatkowe ryzyko dla bezpieczeństwa i ochrony** – dotyczy bezpieczeństwa małoletnich, w szczególności bezpieczeństwa fizycznego, a także wszystkich kwestii związanych z cyberbezpieczeństwem.
- b. **Ryzyko niewłaściwego wykorzystania** – wiąże się z ryzykiem lub szkodami dla małoletnich wynikającymi z niewłaściwego wykorzystania platformy internetowej lub jej funkcji.



⁽¹⁰⁵⁾ Livingstone, S., i Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children* [4C: klasyfikacja ryzyka dla dzieci w internecie] (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>.