

Stanowisko ws. EU Kids Act

Wstęp

Jako organizacje pozarządowe dbające o otwartość i pluralizm środowiska cyfrowego widzimy palącą potrzebę ograniczenia skutków modeli biznesowych, w których najmłodsi użytkownicy aplikacji narażeni są na niebezpieczne treści, inwazyjne profilowanie oraz uzależniające algorytmy rekomendacyjne. Wprowadzenie wiążących zasad projektowania z myślą o bezpieczeństwie użytkowników stanowi krok we właściwym kierunku, jednak ramy te muszą być wyważone, aby ochrona małoletnich nie stała się pretekstem do niebezpiecznego zawężenia praw obywateli i obywaterek do prywatności, rzetelnej informacji i swobodnego uczestnictwa w życiu społecznym.

Bezpieczeństwo w projektowaniu jako fundament regulacji

Popieramy obowiązki dotyczące uzależniających cech projektowych (art. 9), systemów rekomendacji (art. 10) i bezpiecznych ustawień domyślnych (art. 11). Popieramy także ogólny obowiązek uwzględniania bezpieczeństwa na etapie projektowania (art. 8) oraz możliwość uzupełniania przez Komisję listy „ryzykownych” funkcji (art. 6 ust. 6). Te przepisy ograniczają ryzyko, że dostawcy zastąpią zakazane mechanizmy nowymi, nieobjętymi regulacją. Jednak same listy funkcji „ryzykownych”, ujęte w art. 9 i 10, nie są sformułowane odpowiednio szeroko, aby faktycznie zapobiec kompulsywnemu lub nadmiernemu korzystaniu z usług przez małoletnich.

Rekomendujemy, aby Polska w negocjacjach poszerzyła ujęcie „ryzykownych” funkcji w art. 9 i art. 10 w sposób, który uwzględni:

- personalizowanie treści, formy lub momentu przedstawienia oferty handlowej lub komunikatu handlowego na podstawie wynioskowanego stanu emocjonalnego lub psychicznego użytkownika;
- personalizowanie rekomendacji lub funkcji optymalizujących zaangażowanie na podstawie danych behawioralnych lub danych wynioskowanych (danych pośrednich) użytkownika;
- kierowanie lub dostosowywanie ofert handlowych, komunikatów handlowych lub rekomendacji do użytkownika, bądź dostosowywanie ich treści, formy lub momentu przedstawienia na podstawie cech wrażliwych, tj. informacji o podatnościach użytkownika;

- stosowanie jako domyślnego ustawienia usługi personalizacji opartej na danych osobowych innych niż te, które zostały bezpośrednio przekazane przez użytkownika, jak również wymaganie od użytkownika, aby wyłączenie takiej personalizacji polegało na większej liczbie czynności niż jej włączenie;
- zwiększanie częstotliwości lub zmiana momentu wysyłania powiadomień kierowanych do użytkownika, dostosowywanie wyboru lub rankingu treści lub rekomendacji, lub wyświetlanie użytkownikowi komunikatów zachęcających do pozostania na stronie, w przypadku pozyskania przez dostawcę usługi sygnału wskazującego na spadek zaangażowania użytkownika.

Zwracamy również uwagę, że projektowane rozporządzenie de facto pozwala na stosowanie „ryzykownych” (w tym uzależniających) funkcji wobec nastolatków od 15 roku życia oraz osób dorosłych. Tymczasem samo zastosowanie „bramek” (weryfikacja wieku) nie powinno legalizować modelu biznesowego opartego na zaangażowaniu użytkowników za wszelką cenę i eksploataowaniu ich danych. Rekomendujemy, aby Polska w negocjacjach broniła i wzmacniała zasadę „safety by design” oraz wspierała objęcie podobnymi wymogami wszystkich użytkowników w aktach prawnych, nad którymi trwają prace (m.in. w akcie o uczciwości cyfrowej – DFA).

Weryfikacja wieku: warunki, przy których można ją poprzeć

Przepisy wymagające weryfikacji wieku obejmą zarówno dzieci młodsze nastolatki, jak i starszą młodzież oraz dorosłych, bo to oni będą musieli udowodnić, że przekroczyli próg wiekowy. Art. 6 ust. 4 projektu nakazuje dodatkowo, by w ciągu 6 miesięcy dostawcy sprawdzili wiek posiadaczy istniejących kont i wyłączyli konta osób, których wieku „nie można ustalić”. Dotychczas w większości usług wystarczała deklaracja użytkownika. Zmiana dotyczy więc, jak można szacować, kilkudziesiąt milionów osób w Polsce.

Doceniamy, że projekt wybiera infrastrukturę publiczną zamiast komercyjnych pośredników. Art. 28 zakazuje wykorzystywania potwierdzania wieku do identyfikacji, śledzenia, profilowania i reklamy, a ust. 3 stanowi, że każdy środek potwierdzania wieku „musi być dowodem z wiedzą zerową” (*zero-knowledge proof*, ZKP). To rozwiązanie znacznie lepsze niż skanowanie dokumentów przez platformy czy szacowanie wieku na podstawie zdjęcia twarzy, które to rozwiązania są obecnie coraz powszechniej wprowadzane przez firmy. Poprzemy je, jeśli dowody z wiedzą zerową zostaną zaprojektowane i wdrożone tak, by realnie chroniły prywatność. Obecny stan prac budzi jednak wątpliwości:

- Specyfikacja techniczna unijnego rozwiązania traktuje ZKP jako zalecenie, a obowiązkowe jest jedynie wydawanie pakietów jednorazowych poświadczeń. Według

ekspertyz organizacji broniących praw człowieka takie pakiety pozostawiają ślady, które przy współpracy wydawcy i serwisów pozwalają powiązać aktywność z konkretną osobą.

- Szczegółowe wymogi techniczne określi Komisja w aktach wykonawczych (art. 30 ust. 2), czyli poza zwykłą kontrolą parlamentarną.

Dowód z wiedzą zerową chroni moment okazania poświadczenia, ale nie cały system. Wydawca poświadczenia wie, komu je wydał. Prywatność zależy więc od tego, czy wydawca nie dowiaduje się, gdzie i kiedy poświadczenie zostało użyte.

Projekt rozporządzenia pozwala dostawcom internetowych serwisów społecznościowych i usług platformy udostępniania wideo na korzystanie z własnych narzędzi do potwierdzania wieku, „jeżeli są w stanie wykazać, że te rozwiązania spełniają wymogi określone w art. 27 i 28” (art. 29 ust. 4). W naszej ocenie ten wyjątek może być nadużywany przez bardzo duże platformy, o ile nie zostanie on „uszczelniony” lub poddany kontroli odpowiednich organów (np. Komisji Europejskiej), sprawdzających zgodność ze standardami ochrony danych.

Rekomendujemy, aby Polska w negocjacjach:

1. bbroniła wymogu z art. 28 ust. 3 przed osłabieniem i domagała się, by specyfikacje techniczne były z nim zgodne;
2. zabiegała o wpisanie do rozporządzenia zakazu przekazywania wydawcy informacji o użyciu poświadczenia oraz wymogu niepowiązawalności kolejnych użyć;
3. domagała się, by oprogramowanie unijnego systemu weryfikacji wieku i jego krajowych wdrożeń było udostępnione na wolnej licencji, w całości, wraz z częścią serwerową, i podlegało niezależnemu audytowi;
4. zabiegała o doprecyzowanie art. 29 ust. 4, aby zapobiec nadużywaniu tej furtki przez platformy internetowe;
5. zabiegała o zakaz wykorzystywania infrastruktury weryfikacji wieku do innych celów bez odrębnej podstawy w prawie Unii;
6. zagwarantowała, że wprowadzenie weryfikacji wieku nie będzie skutkowało filtrowaniem internetu i blokowaniem dostępu do serwisów anonimizujących takich jak VPN, sieć Tor i inne.

Dostęp bez pośrednictwa Google i Apple

Ministerstwo Cyfryzacji zapowiedziało, że w Polsce weryfikacja wieku będzie działać w aplikacji mObywatel. Obecne wymagania techniczne tej aplikacji, opisane w dokumencie „Informacje o publicznej aplikacji mobilnej mObywatel” (marzec 2026 r.), obejmują:

- system Android „z domyślnie dostępnymi usługami mobilnymi Google” albo iOS;
- instalację wyłącznie ze sklepu Google Play lub App Store;
- system operacyjny bez modyfikacji, co w praktyce wyklucza także alternatywne systemy, takie jak GrapheneOS czy /e/OS, oraz telefony bez usług Google;
- dostęp do numeru IMEI urządzenia.

Wersji na komputer nie ma: logowanie z komputera wymaga zeskanowania kodu QR telefonem. Osoba korzystająca z komputera z systemem Linux, z telefonu nie będącego smartfonem (takiego jak telefony dedykowane dla osób starszych) albo z telefonu bez usług Google nie ma dziś możliwości skorzystania z mObywatela.

Oznacza to, że publiczna infrastruktura cyfrowej tożsamości, która ma chronić prywatność obywateli, wymaga posiadania urządzenia jednej z dwóch amerykańskich korporacji i zgody na ich warunki. Takie samo ryzyko dotyczy rozwiązania unijnego: prototyp zapowiadał atestację urządzeń przez Google Play Integrity i Apple App Attest, co spotkało się z szeroką krytyką. Projekt rozporządzenia dodatkowo dopuszcza przekazywanie sygnału wieku przez dostawców systemów operacyjnych (art. 29 ust. 6). Każde z tych rozwiązań wzmacnia pozycję tych samych firm, których model biznesowy rozporządzenie ma ograniczać.

Problem dotyczy także przejrzystości. Ustawa o aplikacji mObywatel pierwotnie zobowiązywała do publikacji kodu źródłowego (art. 82). Nowelizacja z 2024 r. uzależniła publikację od opinii zespołów CSIRT i ograniczyła ją do zakresu „niezagrażającego bezpieczeństwu” (art. 81a). Fragment kodu opublikowany w grudniu 2025 r. eksperci ds. bezpieczeństwa ocenili jako niewystarczający do sprawdzenia, jak aplikacja przetwarza dane. Bez pełnej jawności kodu nie da się niezależnie potwierdzić, że krajowe wdrożenie spełni wymogi art. 28 projektu.

Jak wskazujemy w raporcie „Cyfrowa racja stanu” (2026), interoperacyjność i otwarte standardy muszą być egzekwowane w praktyce, a nie tylko deklarowane. Rekomendujemy, aby Polska:

1. zabiegała o wpisanie do rozporządzenia zasady neutralności platformowej: unijne rozwiązanie weryfikacji wieku nie może wymagać – bezpośrednio ani pośrednio – usług, sklepu ani atestacji konkretnego producenta systemu operacyjnego;
2. zapewniła możliwość potwierdzenia wieku z komputera z dowolnym systemem operacyjnym, w tym z Linuksem, np. przy użyciu e-dowodu i czytnika, a także w urzędzie, bez smartfona;
3. udostępniła moduł weryfikacji wieku w mObywatelu na wolnej licencji i umożliwiła jego niezależny audyt;
4. przy okazji wdrożenia rozporządzenia usunęła wymóg korzystania z usług Google w aplikacji mObywatel jako całości.

Migranci i migrantki, osoby wykluczone cyfrowo

Art. 31 ust. 5 projektu zobowiązuje państwa członkowskie do zapewnienia bezpłatnego dostępu do unijnego rozwiązania weryfikacji wieku „obywatelom i rezydentom”. Art. 31 ust. 2 wymienia następujące grupy: obywateli i opiekunów oraz małoletnich zamieszkałych na ich terytorium, w tym osób z niepełnosprawnościami, osób o ograniczonym dostępie cyfrowym lub ograniczonych umiejętnościach cyfrowych oraz osób znajdujących się w trudnej sytuacji, takich jak rodziny uchodźcze i wysiedlone. Pozostaje niejasne, czy gwarancja dostępu do środków elektronicznych chroniących prywatność i weryfikujących wiek obejmuje osoby ubiegające się o ochronę międzynarodową, osoby z tymczasowym statusem lub bez uregulowanego pobytu. W Polsce, zgodnie z deklaracjami Ministerstwa, tą metodą ma być mObywatel. Korzystanie z mObywatela wymaga numeru PESEL i potwierdzenia tożsamości przez profil zaufany, e-dowód lub bankowość elektroniczną – jest to droga niedostępna dla osób o nieuregulowanym statusie, takich jak część migrantów zarobkowych, a brak dostępu do platform społecznościowych o globalnym zasięgu i powiązanych z nimi komunikatorów może pogorszyć już trudną sytuację, w której się znajdują.

Polska ma jeden z najwyższych w UE wskaźników wykluczenia cyfrowego. Najbardziej narażone są osoby starsze, uboższe, z niepełnosprawnościami, mieszkające na wsi i w kryzysie bezdomności. W połączeniu z art. 6 ust. 4 oznacza to ryzyko, że część dorosłych straci dostęp do usług, z których dziś korzysta, w tym do kanałów komunikacji z rodziną i społecznością.

Rekomendujemy, aby Polska:

1. zabiegała o doprecyzowanie art. 31 ust. 2 i 5 tak, by prawo do bezpłatnej weryfikacji przysługiwało każdej osobie przebywającej w Unii, niezależnie od statusu pobytowego;
2. zapewniła ścieżkę weryfikacji wieku i odpowiedzialności rodzicielskiej na podstawie dokumentów zagranicznych, w urzędzie i bez danych biometrycznych;
3. przed wdrożeniem przeprowadziła ocenę skutków dla grup zagrożonych wykluczeniem tak, by wprowadzane mechanizmy dot. weryfikacji wieku, jeśli zostaną przyjęte, były dostępne dla każdej osoby przebywającej w Unii, niezależnie od statusu pobytowego, kompetencji cyfrowych, sytuacji rodzinnej.
4. Zabiegała o wydłużenie okresu przewidzianego w art. 6 ust. 4 do 12 miesięcy.

Kto sfinansuje infrastrukturę

Wydawanie poświadczeń wieku i odpowiedzialności rodzicielskiej oraz utrzymanie infrastruktury sfinansują państwa członkowskie (art. 31), a korzystać z niej będą prywatne platformy. Oplata nadzorcza (art. 36) odprowadzana przez bardzo duże platformy pokrywa koszty nadzoru Komisji, ale nie koszty krajowych systemów. Rekomendujemy, aby Polska zabiegała

o mechanizm, w którym wszyscy dostawcy usług internetowych wykorzystujących uzależniające funkcjonalności lub śledzenie i profilowanie w celach reklamowych współfinansują infrastrukturę, która ma ograniczać skutki tego modelu biznesowego.

Dostęp do wiedzy

Internet powstał jako globalna przestrzeń wymiany myśli, nauki, kultury oraz zasobów wiedzy z domeny publicznej, które stanowią wspólną własność społeczeństwa. Doceniamy opisane w projekcie wyłączenie z obowiązku weryfikacji niekomercyjnych platform, których treści mają charakter edukacyjny, naukowy i informacyjny – wyłączenie to nie obejmuje jednak otwartych repozytoriów wiedzy i kultury oraz inicjatyw oddolnych, które nie są encyklopedyczne lub powiązane z organami publicznymi czy formalnymi organizacjami oświaty. Co istotne, przepisy powinny uwzględniać prawo takich projektów do zrównoważonego finansowania, dopuszczając ich komercjalizację do określonego progu skali działalności lub przychodów. Mechanizm progowy uniemożliwiłby wykorzystanie luki „treści kultury” przez większe podmioty komercyjne, jednocześnie chroniąc kreatywny, otwarty, ale i nie bezkosztowy charakter cyfrowego ekosystemu.

Powszechny, nieograniczony dostęp do cyfrowych dóbr wspólnych oraz możliwość ich współtworzenia nie mogą stać się przypadkową ofiarą walki z inwazyjnymi praktykami dużych firm technologicznych – infrastruktura internetu jako takiego nie może być traktowana na tej samej zasadzie, co komercyjne media społecznościowe. Wymóg legitymowania się cyfrowym poświadczeniem tożsamości tworzy barierę wejścia, która może zniechęcić lub uniemożliwić dostęp do materiałów, a nawet uniemożliwić tworzenie tych zasobów, gdy opierają się one na modelu wspólnej, społecznej produkcji treści.

Nowe przepisy nie powinny nakładać nieproporcjonalnych obowiązków w zakresie moderacji treści, audytów zgodności czy wprowadzania bramek dostępowych, które zmuszałyby do zbierania większej ilości danych o użytkownikach niż jest to realnie potrzebne.

Sygnatariuszki

- Polska Sieć Ekonomii
- Fundacja Centrum Cyfrowe
- Fundacja Panoptykon