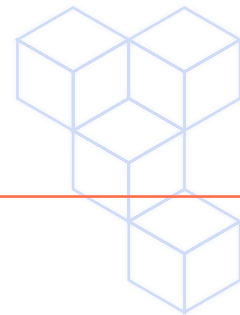


Akt o usługach cyfrowych (Digital Services Act)

**Jak platformy
internetowe powinny
chronić dzieci i młodzież
w internecie**

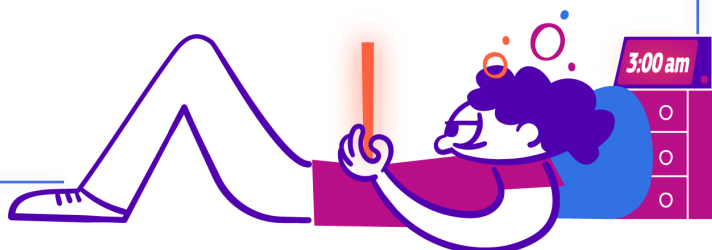


Czego dotyczy akt o usługach cyfrowych (Digital Services Act – DSA)?



Platformy internetowe odgrywają ważną rolę w codziennym życiu dzieci i młodzieży, zarówno jako miejsce spotkań ze znajomymi, oglądania filmów, grania w gry, jak i zdobywania wiedzy czy rozwijania pasji. Korzystanie z internetu wiąże się jednak również z zagrożeniami. Wśród nich znajdziemy m.in.:

- ▶ doświadczanie przykrych sytuacji w sieci,
- ▶ nawiązanie kontaktu z osobami, które mają złe intencje,
- ▶ narażenie na szkodliwe treści, które mogą wywołać dyskomfort, strach lub niepokój,
- ▶ poczucie przymusu, by coś kupić,
- ▶ udział w ryzykownych wyzwaniach,
- ▶ trudność z odłożeniem telefonu lub wyłączeniem konsoli.



Aby zwiększyć bezpieczeństwo w internecie, w 2022 r. Unia Europejska (UE) uchwaliła akt o usługach cyfrowych. Akt ten ma zastosowanie do platform internetowych (europejskich i nieeuropejskich) dostępnych na terenie UE. Ma on na celu zapewnienie wszystkim użytkownikom internetu – w tym dzieciom i młodzieży – ochrony przed powyższymi i innymi zagrożeniami oraz ochronę praw podstawowych w internecie.

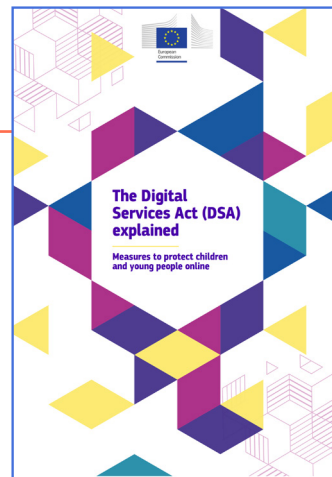
Wszystkie platformy internetowe muszą przestrzegać tego aktu prawnego i dbać o bezpieczeństwo użytkowników korzystających z nich na terenie UE.



W jaki sposób akt o usługach cyfrowych chroni dzieci i młodzież w internecie

Na podstawie aktu o usługach **cyfrowych platformy internetowe muszą zapewnić małoletnim wysoki poziom prywatności, bezpieczeństwa i ochrony podczas korzystania z oferowanych przez nie usług**. Oznacza to, że dzieci i młodzież powinny mieć poczucie, że są chronione i bezpieczne podczas korzystania z aplikacji, mediów społecznościowych i gier, które podlegają przepisom tego aktu. Największe platformy, które mają ponad 45 mln użytkowników w UE, takie jak TikTok, Instagram i Snapchat, mają obowiązek rozpoznawania i oceniania sytuacji, które potencjalnie mogą negatywnie wpływać na dzieci i młodzież korzystające z ich usług.

W lipcu 2025 r. Komisja Europejska opublikowała wytyczne dotyczące ochrony małoletnich, których celem jest ułatwienie wszystkim platformom zrozumienia, jakie kroki trzeba podjąć, aby zapewnić dzieciom i młodzieży przyjazne i bezpieczne środowisko online. Niniejsza broszura wyjaśnia, na czym polegają te wytyczne.



Chcesz dowiedzieć się więcej o akcie o usługach cyfrowych? Przeczytaj tę broszurę na temat działań chroniących dzieci i młodzież w internecie.

Oto co znajdziesz w środku

1. Kto musi przestrzegać wytycznych w zakresie ochrony małoletnich	4
2. Jakie są najważniejsze założenia	5
3. Zalecenia	6
a. Ocena ryzyka: każda platforma wiąże się z innymi zagrożeniami	6
b. Kontrola wieku: w jaki sposób platformy sprawdzają wiek użytkowników	6
c. Rejestracja: poznanie zasad, praw i obowiązków dla świadomego korzystania	10
d. Ustawienia konta: prywatność i bezpieczeństwo, które możesz kontrolować	11
e. Interfejsy: projektowanie platform w taki sposób, aby były proste i bezpieczne w użyciu	13
f. Systemy rekomendacji i funkcje wyszukiwania: pomaganie dzieciom i młodzieży w zachowaniu kontroli	14
g. Działania reklamowe: pomaganie dzieciom i młodzieży w zrozumieniu, co jest promowane i sprzedawane	15
h. Moderacja: dbanie o bezpieczeństwo i wzajemny szacunek na platformach	16
i. Zgłaszanie: ułatwianie zgłaszania problemów i uzyskiwania pomocy	17
j. Narzędzia dla rodziców i opiekunów	18
4. Kto dba o przestrzeganie przepisów aktu o usługach cyfrowych	19
5. Co dalej	19
Gdzie znajdziesz więcej informacji i uzyskasz pomoc	24

Pamiętaj, że niniejsza publikacja ma charakter wyłącznie informacyjny i nie jest dokumentem prawnym.

1. Kto musi przestrzegać wytycznych w zakresie ochrony małoletnich

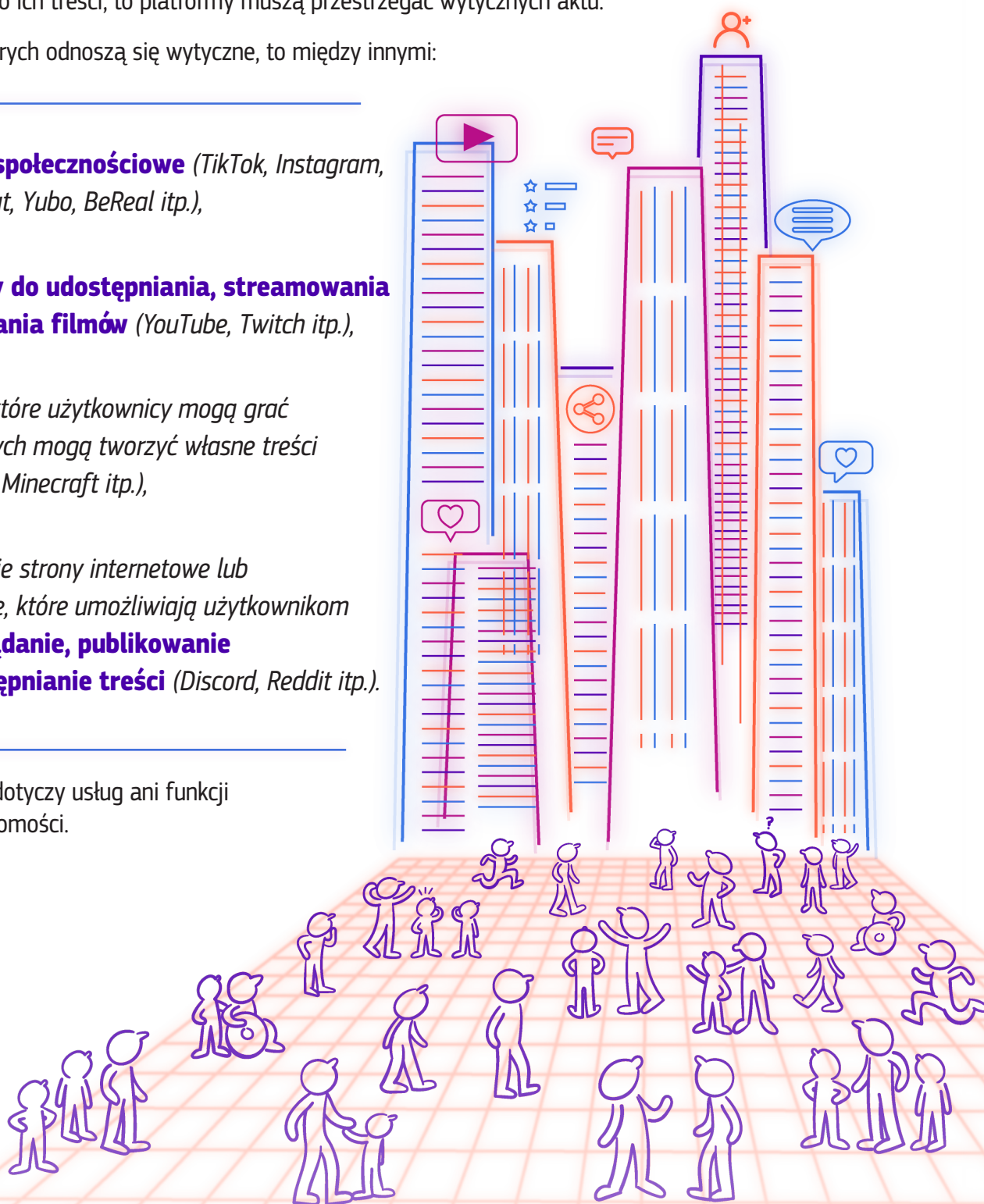
Jeśli z platformy korzystają dzieci i młodzież – lub jeśli istnieje prawdopodobieństwo, że mogą uzyskać do niej dostęp – platforma **musi** przestrzegać postanowień aktu o usługach cyfrowych i wytycznych w zakresie ochrony małoletnich.

Strony internetowe przeznaczone dla dorosłych nie mogą jedynie zapisać w swoich regulaminach, że „osoby małoletnie nie mogą z nich korzystać”, a tym samym pomijać fakt, że dzieci i tak mogą tam wejść. Jeśli istnieje prawdopodobieństwo, że młodsze osoby mogą uzyskać dostęp do ich treści, to platformy muszą przestrzegać wytycznych aktu.

Platformy, do których odnoszą się wytyczne, to między innymi:

- ▶ **media społecznościowe** (*TikTok, Instagram, Snapchat, Yubo, BeReal itp.*),
- ▶ **serwisy do udostępniania, streamowania i oglądania filmów** (*YouTube, Twitch itp.*),
- ▶ **gry**, w które użytkownicy mogą grać i w których mogą tworzyć własne treści (*Roblox, Minecraft itp.*),
- ▶ **wszystkie strony internetowe lub aplikacje, które umożliwiają użytkownikom przeglądanie, publikowanie i udostępnianie treści** (*Discord, Reddit itp.*).

Uwaga: DSA nie dotyczy usług ani funkcji prywatnych wiadomości.



2. Jakie są najważniejsze założenia

Wytyczne opierają się na trzech głównych koncepcjach:

1. Prawa dzieci są najważniejsze

Platformy powinny szanować prawa dzieci i zawsze kierować się ich dobrem. Prawa te obejmują:

- ▶ *ochronę,*
- ▶ *brak dyskryminacji,*
- ▶ *włączenie,*
- ▶ *prywatność,*
- ▶ *dostęp do informacji i edukacji,*
- ▶ *wolność wypowiedzi,*
- ▶ *uczestnictwo.*

Oznacza to projektowanie, tworzenie i zarządzanie takimi usługami internetowymi, które są bezpieczne i zapewniają prywatność.

2. Bezpieczeństwo na etapie projektowania

Platformy nie powinny czekać aż problemy się pojawią. Prywatność i bezpieczeństwo podczas korzystania z ich usług powinny być zapewnione od samego początku, a dostępne funkcje dostosowane do różnych grup wiekowych i etapów rozwoju dzieci.

3. Zrozumienie potrzeb użytkowników

Platformy muszą dokładnie przeanalizować, w jaki sposób dzieci i młodzież korzystają z ich usług oraz jakie zagrożenia i problemy mogą się pojawić, na przykład:

- ▶ *cyberprzemoc,*
- ▶ *treści, które mogą być nieodpowiednie dla ich wieku,*
- ▶ *zbyt długie korzystanie.*

Następnie muszą znaleźć sposoby i wdrożyć rozwiązania, które pomogą ograniczyć takie sytuacje.



3. Zalecenia

Przyjrzyjmy się zaleceniom, których platformy internetowe muszą przestrzegać, aby chronić dzieci i młodzież w internecie.

a. Ocena ryzyka: każda platforma wiąże się z innymi zagrożeniami

Wytyczne zalecają, aby platformy **regularnie kontrolowały**, czy ich treści są **bezpieczne i odpowiednie dla dzieci i młodzieży**, oraz aby potrafiły wyjaśnić, w jaki sposób dbają o ich dobro. Oznacza to konieczność wypracowania kompromisu między:

- ▶ umożliwieniem dzieciom i młodzieży dzielenia się treściami, pomysłami i refleksjami,
- ▶ daniem im szansy na odkrywanie, zabawę i uczenie się nowych rzeczy w internecie...

... a jednocześnie dbaniem o ich bezpieczeństwo!



Po zidentyfikowaniu zagrożeń platformy powinny reagować, wprowadzając skuteczne rozwiązania – bez ograniczania możliwości i korzyści, jakie dzieci mogą czerpać z internetu.

b. Kontrola wieku: w jaki sposób platformy sprawdzają wiek użytkowników

Aby zapewnić większe bezpieczeństwo platform i chronić dzieci i młodzież przed treściami, które nie są dla nich przeznaczone, konieczna jest wiedza, czy użytkownicy są **w odpowiednim wieku**, aby uzyskać dostęp do danych treści.

Tutaj pojawia się kwestia **kontroli wieku**.

Kontrola wieku oznacza wykorzystanie narzędzi do:

- ▶ ustalenia lub oszacowania wieku użytkownika lub
- ▶ potwierdzenia, czy dana osoba jest starsza lub młodsza niż określony wiek.



Czy wiesz, że...

Aby korzystać z aplikacji TikTok, Snapchat, Instagram, BeReal i Steam, musisz mieć co najmniej 13 lat?



Rodzaje kontroli wieku

Istnieją trzy główne sposoby sprawdzania wieku użytkownika przez platformy:

1. Własna deklaracja

Wpisujesz swoją datę urodzenia lub klikasz „Tak, mam ukończone 13 lat” lub „Tak, mam ukończone 18 lat”. Jest to rozwiązanie szybkie, ale podatne na oszustwa, więc **nie jest ono wystarczająco skuteczne ani niezawodne**.

2. Oszacowanie wieku

Technologia pozwala ocenić Twój wiek na podstawie takich czynników, jak:

- > analiza twarzy,
- > styl pisania,
- > Twoje zainteresowania.

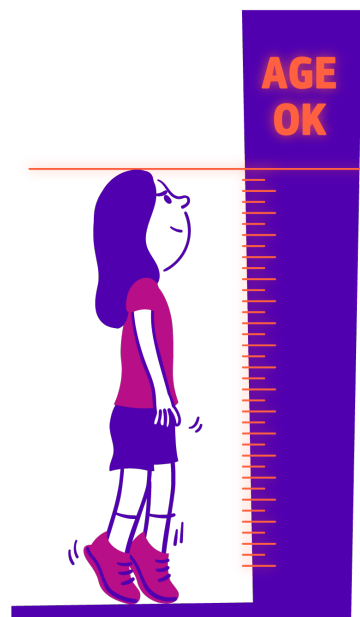
Nie jest to rozwiązanie idealne – nie zawsze dokładnie określa wiek i może **naruszać** Twoją prywatność.

3. Weryfikacja wieku

To **najdokładniejsza** metoda. Weryfikacja wieku odbywa się na podstawie:

- > oficjalnych dokumentów, takich jak paszport,
- > zaufanych identyfikatorów cyfrowych, takich jak identyfikator rządowy (np. PESEL) lub aplikacja mObywatel czy europejski portfel tożsamości cyfrowej.

Ta ostatnia metoda **zapewnia ochronę prywatności**, ponieważ użytkownicy mogą potwierdzić swój wiek bez ujawniania żadnych innych danych osobowych.



EU Digital Identity
Wallet

Czym jest europejski portfel tożsamości cyfrowej? To bezpłatna aplikacja, która ułatwi mieszkańcom Europy (jej wprowadzenie planowane jest w 2026 r.):

- ▶ bezpieczne przechowywanie ważnych dokumentów w jednym miejscu,
- ▶ potwierdzanie tożsamości zarówno w internecie, jak i poza nim.

To coś w rodzaju cyfrowego plecaka na dowód osobisty i inne ważne dokumenty.



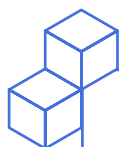
3. Zalecenia

Platformy internetowe powinny:

- ▶ wyjaśniać, na czym polega sprawdzanie wieku, w sposób **zrozumiały** dla dzieci i młodzieży,
- ▶ pytać o wiek tylko wtedy, gdy jest to **naprawdę konieczne** dla zapewnienia bezpieczeństwa użytkowników,
- ▶ stosować **najprostszą metodę**, która się sprawdza, bez proszenia o więcej informacji niż to konieczne,
- ▶ dopilnować, aby wszystkie metody sprawdzania wieku były **dokładne, wiarygodne i trudne do obejścia**,
- ▶ oferować **więcej niż jedną metodę**, aby nikt nie był wykluczony,
- ▶ umożliwić użytkownikom **odwołanie się**, jeśli ich wiek został błędnie oszacowany.



Jakiej metody powinny używać platformy?



Kontrola wieku wydaje się nieco skomplikowana, prawda? Ten przewodnik na temat kontroli wieku pomoże Ci to lepiej zrozumieć.





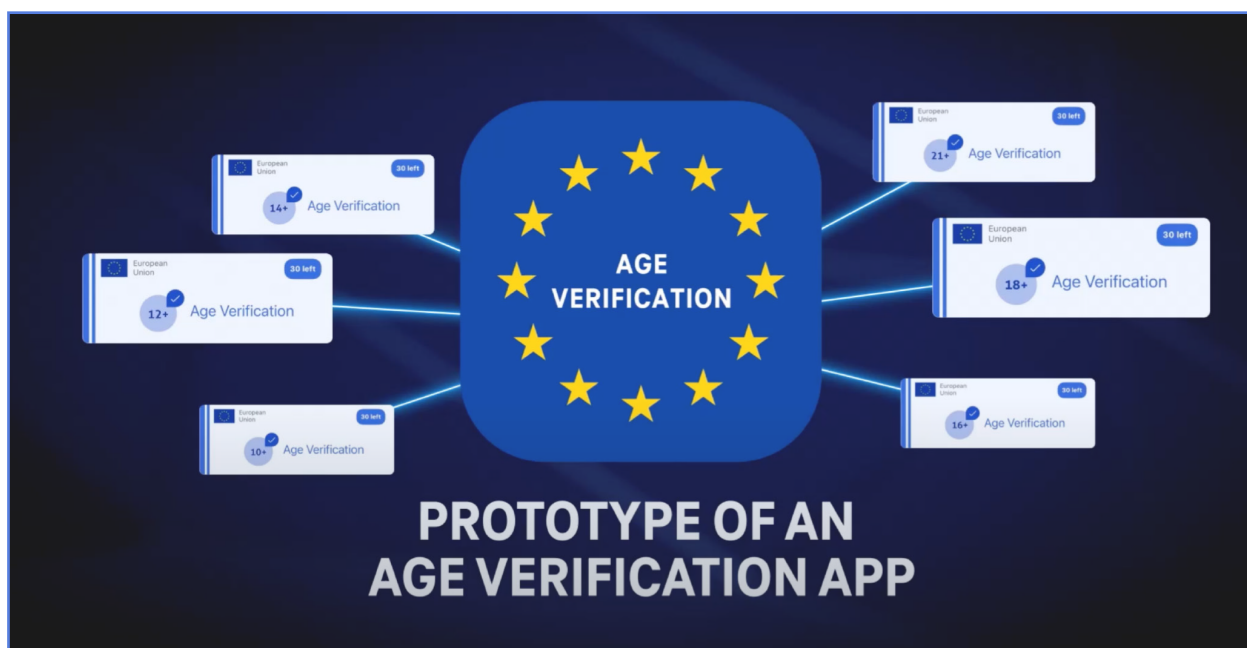
Czy aplikacja naprawdę potrafi zweryfikować Twój wiek?

Tak! Komisja Europejska pracuje nad rozwiązaniem odpowiednim dla Ciebie!
W lipcu 2025 r. przedstawiła **konceptę aplikacji do weryfikacji wieku**

Została ona zaprojektowana tak, aby:

- ▶ *była przyjazna dla użytkowników,*
- ▶ *umożliwiała użytkownikom udowodnienie, że mają ukończone 18 lat,*
- ▶ *nie wymagała podawania żadnych innych danych osobowych.*

Dzięki temu dostęp do niektórych treści w internecie
będzie **bezpieczny i odpowiedni do wieku użytkowników**.



Ciekawi Cię podejście UE do weryfikacji wieku?
Zeskanuj kod QR, aby dowiedzieć się więcej!



3. Zalecenia

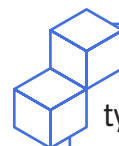
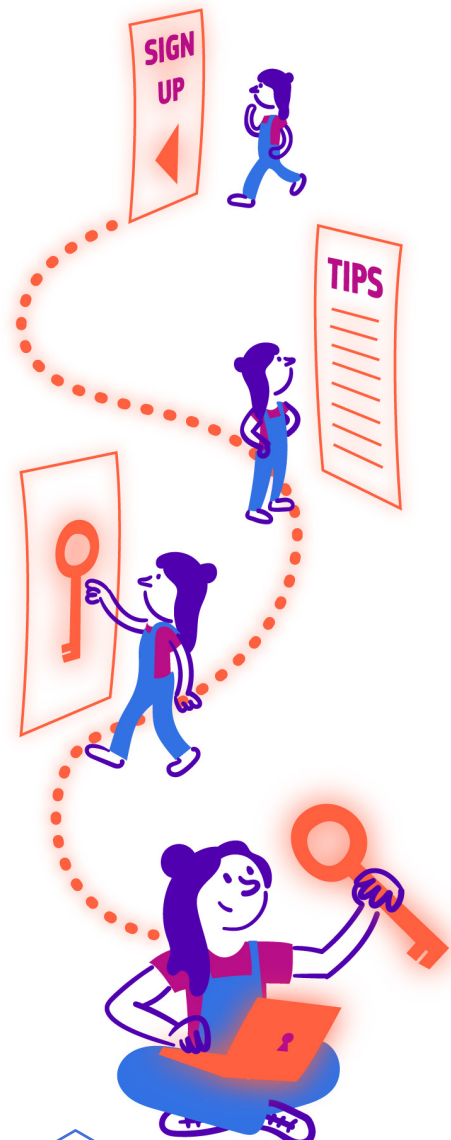
c. Rejestracja: poznanie zasad, praw i obowiązków dla świadomego korzystania

Kiedy platforma prosi użytkowników o zarejestrowanie się, to jest to dobry moment, by:

- ▶ udostępnić ważne **informacje dotyczące bezpieczeństwa**,
- ▶ udzielić **wskazówek edukacyjnych**,
- ▶ upewnić się, że użytkownik jest **w odpowiednim wieku** do korzystania z usługi.

Aby móc to zrobić, platformy muszą:

- ▶ **jasno wytłumaczyć**, dlaczego rejestracja jest tak ważna i jakie daje korzyści,
- ▶ zapewnić **prosty i dostępny proces rejestracji**, zwłaszcza dla dzieci i młodzieży ze specjalnymi potrzebami lub niepełnosprawnościami,
- ▶ unikać zachęcania do rejestracji osób, które są za młode,
- ▶ umożliwić dzieciom **łatwe wylogowanie** się lub **usunięcie konta** w dowolnej chwili,
- ▶ wykorzystać moment rejestracji, by wyjaśnić **kluczowe zabezpieczenia**, takie jak:
 - > ustawienia prywatności,
 - > domyślne zabezpieczenia,
 - > narzędzia zgłaszania.
- ▶ pomagać dzieciom i młodzieży zrozumieć:
 - > jakie **narzędzia bezpieczeństwa są dostępne**,
 - > jak i gdzie **szukać pomocy** w razie potrzeby.



Rejestracja to nie tylko tworzenie konta. To także szansa dla platformy, aby zapewnić młodym użytkownikom **bezpieczny** start dzięki **dostępowi do informacji** i możliwości **samodzielnej kontroli**.

d. Ustawienia konta: prywatność i bezpieczeństwo, które możesz kontrolować

Ustawienia konta mogą pomóc dzieciom, młodzieży i ich rodzicom w kontrolowaniu ich aktywności w internecie – np. w zakresie tego, jakie dane osobowe są widoczne dla innych lub kto może się z nimi skontaktować.

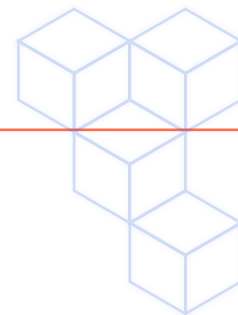
Ponieważ większość osób nie zmienia ustawień domyślnych, platformy muszą zadbać o to, aby **od samego początku zapewniały one prywatność, bezpieczeństwo i ochronę.**

Co powinny obejmować domyślne ustawienia?

- ▶ **Ograniczenie widoczności i kontaktów:** kontrolę tego, kto może obserwować dziecko lub nastolatka i kto może wysłać im wiadomości.
- ▶ **Domyślne wyłączenie funkcji,** z których korzystanie może wiązać się z pewnymi ryzykami, takich jak:
 - > geolokalizacja,
 - > automatyczne odtwarzanie filmów,
 - > mikrofon i aparat,
 - > synchronizacja kontaktów,
 - > śledzenie.
- ▶ **Zapobieganie** przeglądaniu lub pobieraniu treści przez nieznanym.
- ▶ **Udostępnianie informacji kontaktowych** (np. adresu e-mail lub numeru telefonu) **tylko za wyraźną zgodą.**
- ▶ **Zarządzanie powiadomieniami:** **wyłączenie powiadomień typu „push” lub alertów** od określonych użytkowników lub aplikacji w nocy.
- ▶ **Ograniczanie nadmiernego używania** poprzez możliwość wyłączenia takich funkcji, jak:
 - > liczniki polubień i reakcji,
 - > funkcja „...pisze”,
 - > potwierdzenie przeczytania wiadomości.
- ▶ **Ochronę zdrowia psychicznego:** wyłączenie filtrów obrazów, które mogą negatywnie wpływać na postrzeganie własnego ciała lub samoocenę.



3. Zalecenia



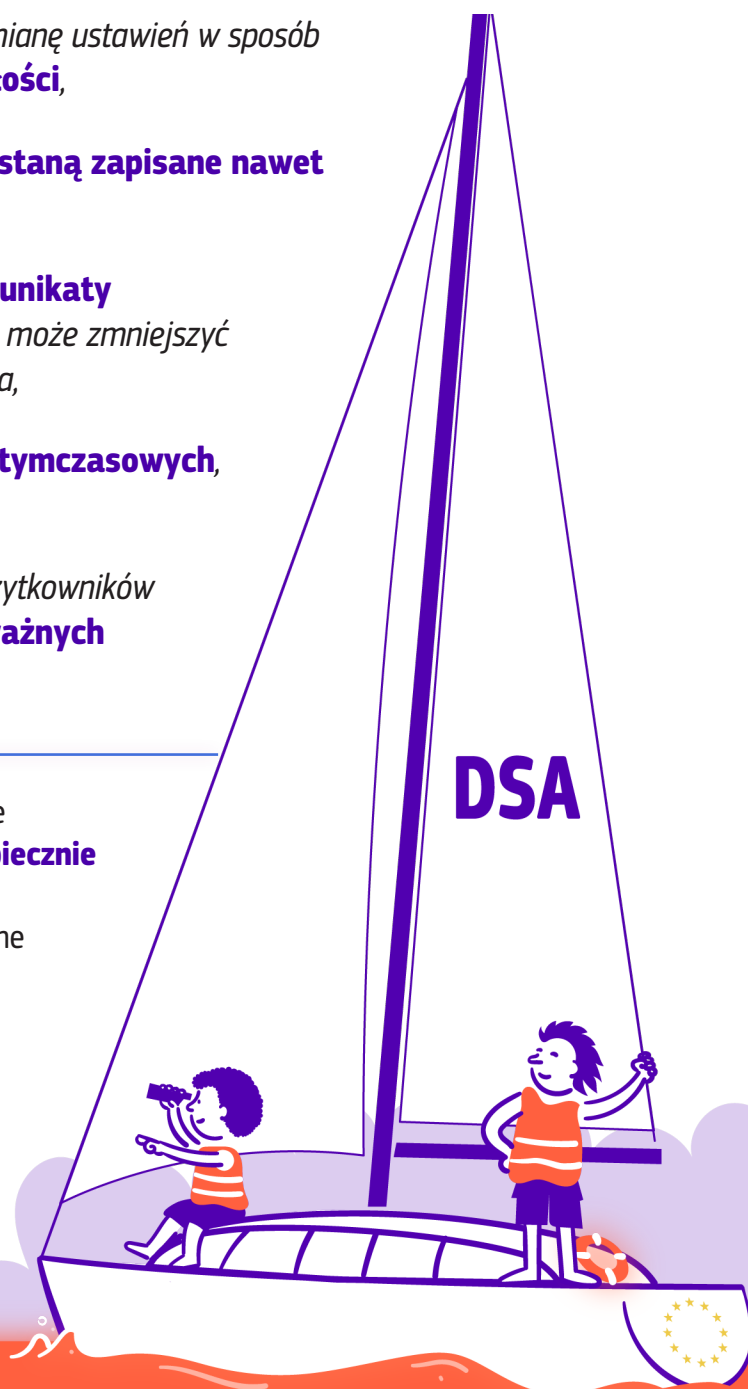
Przekazanie kontroli dzieciom i młodzieży – ze wsparciem dorosłych

Warto zachęcać dzieci do zachowania ustawień dotyczących prywatności, bezpieczeństwa i ochrony. Jeśli jednak chcą **zmienić wybrane ustawienia**, powinny mieć możliwość zrobienia tego w sposób bezpieczny i odpowiedni do ich wieku.

Platformy muszą:

- ▶ umożliwić młodym użytkownikom zmianę ustawień w sposób dostosowany do ich **wieku** i **dojrzałości**,
- ▶ zagwarantować, że ich wybory **pozostaną zapisane nawet po aktualizacji platformy**,
- ▶ wyświetlać jasne i **zrozumiałe komunikaty z ostrzeżeniami**, jeśli dana zmiana może zmniejszyć prywatność lub bezpieczeństwo konta,
- ▶ **umożliwić wprowadzanie zmian tymczasowych**, a nie tylko trwałych,
- ▶ **od czasu do czasu prosić młodych użytkowników o sprawdzenie i potwierdzenie ważnych ustawień.**

Dlaczego jest to ważne? Ustawienia domyślne pomagają dzieciom i młodzieży czuć się **bezpiecznie i mieć kontrolę nad kontem**, bez poczucia przytłoczenia lub narażania się na niepotrzebne ryzyko.



e. Interfejsy: projektowanie platform w taki sposób, aby były proste i bezpieczne w użyciu

Interfejs to inaczej wygląd i układ platformy internetowej – to, co widzisz na ekranie i w jaki sposób z niej korzystasz. Dobrze zaprojektowany interfejs może pomóc dzieciom i młodzieży **bezpiecznie korzystać z internetu, poczuć się pewnie i czerpać radość z czasu spędzanego w sieci**.

Aby zapobiec nadmiernemu przebywaniu w internecie i uzależnieniu oraz ułatwić wylogowanie się, platformy powinny unikać takich funkcji, jak:

- ▶ *niekończące się przewijanie, czyli gdy strona zostanie przewinięta do samego dołu, następuje automatyczne odświeżenie i pojawia się nowa treść,*
- ▶ *„przeciągnij, aby odświeżyć”,*
- ▶ *ciągłe powiadomienia,*
- ▶ *automatyczne odtwarzanie filmów,*
- ▶ *codzienne wirtualne nagrody, „streak” (tzn. nieprzerwany ciąg dni, w których użytkownik wykonywał określoną aktywność w aplikacji) lub punkty, które zachęcają dzieci do uruchamiania aplikacji lub gry każdego dnia.*



Platformy muszą oferować:

- ▶ *narzędzia pomagające dzieciom i młodzieży **zarządzać czasem spędzonym w internecie**, takie jak przypomnienia o zrobieniu przerwy,*
- ▶ **łatwy dostęp** do ustawień bezpieczeństwa oraz **proste i zrozumiałe** narzędzia do zgłaszania problemów i przekazywania opinii,
- ▶ **dostępność** dla wszystkich, w tym dla dzieci i młodzieży z niepełnosprawnościami lub specjalnymi potrzebami,
- ▶ wyraźne **ostrzeżenia**, gdy dzieci i młodzież korzystają z funkcji wykorzystujących **sztuczną inteligencję**.



3. Zalecenia

f. Systemy rekomendacji i funkcje wyszukiwania: pomaganie dzieciom i młodzieży w zachowaniu kontroli

Czy nie zastanawia Cię to, skąd aplikacje mediów społecznościowych lub platformy z Twoimi ulubionymi serialami zawsze wiedzą, co zaproponować jako kolejne?

Systemy rekomendacji decydują o tym, jakie treści lub sugestie kontaktów pojawiają się w kanałach użytkowników – w tym na stronach *explore* (odkrywaj) – na podstawie tego, co wcześniej polubili, obejrzeli, kliknęli lub postanowili obserwować.

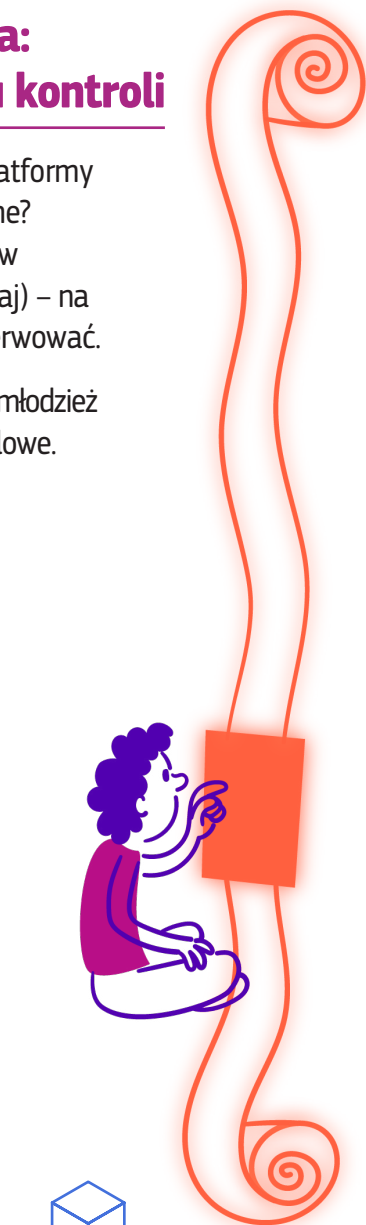
Mimo że wydaje się to być pomocne, może również prowadzić do tego, że dzieci i młodzież zobaczą szkodliwe lub nieodpowiednie obrazy, filmy, posty lub produkty handlowe.

Platformy powinny:

- ▶ pokazywać wyłącznie treści **dostosowane do wieku**,
- ▶ ograniczać ilość **danych gromadzonych i wykorzystywanych** do tworzenia rekomendacji,
- ▶ traktować **priorytetowo decyzje i opinie użytkowników**, takie jak:
 - > „Pokazuj mi mniej/więcej podobnych treści”,
 - > „Nie chcę tego oglądać”,
 - > „Nie interesuje mnie to”,
- ▶ unikać nadmiernego polegania na informacjach **wyrażonych pasywnie**, takich jak czas spędzony na oglądaniu lub przeglądaniu,
- ▶ wyjaśniać, **dlaczego dana treść została polecona** i jak można to zmienić,
- ▶ umożliwiać użytkownikom całkowite i trwałe **zresetowanie ich kanału**,
- ▶ ułatwiać **zgłaszanie niepożądanych treści** – i dbać o to, aby zgłoszenia faktycznie miały wpływ na proponowane materiały,
- ▶ projektować ustawienia systemu rekomendacji tak, by były zrozumiałe, **przyjazne i łatwo dostępne dla dzieci**.

Funkcje wyszukiwania powinny:

- ▶ blokować niebezpieczne słowa i hasztagi,
- ▶ ułatwiać dzieciom i młodzieży wybór tego, co ich najbardziej interesuje.



Systemy rekomendacji powinny dawać dzieciom więcej możliwości, a nie je przytłaczać. Przekazanie młodym użytkownikom kontroli nad tym, co oglądają, pomaga zapewnić im **bezpieczniejsze i bardziej pozytywne doświadczenia w internecie**.

g. Działania reklamowe: pomaganie dzieciom i młodzieży w zrozumieniu, co jest promowane i sprzedawane

Dzieci i młodzież – podobnie jak dorośli – nie zawsze zdają sobie sprawę, że coś w internecie jest:

- ▶ reklamą,
- ▶ ukrytą reklamą,
- ▶ płatnym postem influencera.

Trudno jest też dostrzec, w jaki sposób aplikacje, gry lub strony internetowe próbują nas skłonić do spędzania więcej czasu online lub wydawania więcej pieniędzy. Może to prowadzić do niepotrzebnych zakupów, nadmiernych wydatków lub nawyków, których trudno się pozbyć.

Platformy muszą:

- ▶ wyraźnie i konsekwentnie **oznaczać wszystkie treści reklamowe i sponsorowane** – w tym lokowanie produktów przez influencerów,
- ▶ regularnie weryfikować sposób oznaczania reklam oraz konsultować z dziećmi i opiekunami, na ile oznaczenia są **czytelne i skuteczne**,
- ▶ unikać reklamowania dzieciom i młodzieży produktów i usług, które mogą mieć negatywny wpływ na ich **prywatność i bezpieczeństwo**,
- ▶ otwarcie informować o kosztach i konsekwencjach:
 - > **zakupów w aplikacjach**,
 - > **wirtualnych walut lub tokenów**,
 - > innych **transakcji**,
- ▶ unikać taktyk wywierania presji, takich jak:
 - > **odliczanie czasu**,
 - > komunikaty „**kup teraz**”,
- ▶ blokować dostęp do wszelkich funkcji posiadających elementy **hazardu**, takich jak np. **skrzynki z łupami w grach** (tzw. loot box),
- ▶ pilnować, aby „bezpłatne” produkty i usługi nie wiązały się z **ukrytymi zakupami**,
- ▶ dbać o to, aby reklamy były **dostosowane do wieku**,
- ▶ dostosować algorytmy tak, aby **dzieci nie oglądały zbyt często lub zbyt wielu reklam**.



Co oznaczają te pojęcia?

Lokowanie produktu polega na pokazywaniu marki lub produktu w materiale wideo lub poście w ramach płatnej reklamy.

Skrzynka z łupami to cyfrowy przedmiot, który oferuje losowe nagrody, często wykorzystywany w grach.

Zakupy w aplikacji to usługa, którą kupujesz w aplikacji, np. dodatkowe funkcje, więcej żyć, nowe skórki lub wirtualne monety.

Dlaczego jest to ważne? Środki te mogą pomóc chronić dzieci i młodzież przed **nakłanianiem ich lub wywieraniem na nie presji**, aby wydały pieniądze, gdy nie chcą tego robić.

3. Zalecenia

h. Moderacja: dbanie o bezpieczeństwo i wzajemny szacunek na platformach

Moderacja oznacza **sprawdzanie i usuwanie treści lub kont**, które mogą negatywnie wpływać na prywatność, bezpieczeństwo i ochronę dzieci i młodzieży, w tym na ich ogólne samopoczucie fizyczne i psychiczne.

Jest to ważne narzędzie do ochrony użytkowników i zapobiegania poważnym zagrożeniom, takim jak nękanie, narażenie na szkodliwe treści lub nagabywanie dzieci w celach seksualnych.

Platformy powinny:

- ▶ jasno określić, co należy rozumieć jako **szkodliwe treści i niebezpieczne zachowania**,
- ▶ stosować skuteczne metody **szybkiego usuwania szkodliwych lub nielegalnych treści i kont**,
- ▶ szkolić moderatorów w rozpoznawaniu zagrożeń dla dzieci i młodzieży, takich jak **nagabywanie dzieci w celach seksualnych lub niebezpieczne wyzwania**,
- ▶ **natychmiast** usuwać nielegalne lub szkodliwe treści,
- ▶ stosować narzędzia **zapobiegające tworzeniu lub udostępnianiu przez użytkowników szkodliwych treści generowanych przez sztuczną inteligencję**,
- ▶ **regularnie weryfikować i ulepszać** swoje systemy moderacji.



Moderacja to nie tylko usuwanie treści – to tworzenie bezpieczniejszej i bardziej przyjaznej przestrzeni w sieci dla wszystkich.



Prawidłowa moderacja pozwala stworzyć przestrzeń, w której dzieci i młodzież czują się **bezpieczne, szanowane i wspierane**.

i. Zgłaszanie: ułatwianie zgłaszania problemów i uzyskiwania pomocy

Czasami w sieci zdarzają się nieprzyjemne sytuacje. Możesz natknąć się na niepokojące treści, doświadczyć nękania lub nie czuć się bezpiecznie. Dlatego ważne jest, aby platformy umożliwiały **wszystkim łatwe zgłaszanie problemów i uzyskiwanie pomocy**.

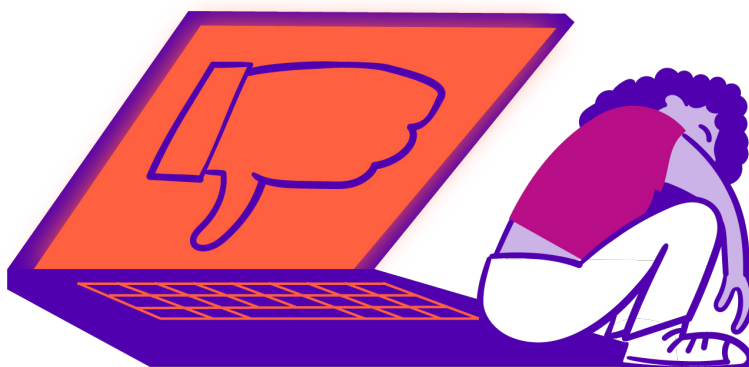
Platformy muszą:

- ▶ zapewnić wszystkim użytkownikom (w tym osobom z niepełnosprawnościami) **proste i szybkie metody zgłaszania** nadużyć, nękania lub szkodliwych treści,
- ▶ umożliwić użytkownikom **blokowanie, wyciszenie lub ograniczanie** komentarzy i interakcji z innymi użytkownikami,
- ▶ zadbać o to, aby użytkownicy nie byli **automatycznie dodawani do grup** – dołączenie do grupy powinno nastąpić dopiero po przyjęciu zaproszenia,
- ▶ udzielać **szybkich i pomocnych odpowiedzi**, gdy użytkownicy zgłaszają problem, oraz informacji zwrotnych na temat tego, co się stało.



Potrzebujesz pomocy
w zgłoszeniu
niepokojących treści?
Sieć centrów
bezpieczniejszego
internetu w całej
Europie może Ci
pomóc!

Centra zapewnią Ci
wsparcie, praktyczną
pomoc, porady
i kogoś, kto cię
wysłucha, niezależnie
od tego, o czym
chcesz porozmawiać.



3. Zalecenia

j. Narzędzia dla rodziców i opiekunów

Rodzice i opiekunowie mogą pomóc dzieciom i nastolatkom w bezpiecznym korzystaniu z internetu. Platformy mogą oferować narzędzia, które temu sprzyjają, **nie pozbawiając młodych ludzi ich praw ani niezależności**.

Jeśli platformy zdecydują się na wprowadzenie narzędzi kontroli rodzicielskiej jako uzupełnienie obowiązkowych zabezpieczeń, narzędzia te powinny:

- ▶ *opierać się na **komunikacji i upodmiotowieniu**, a nie kontroli,*
- ▶ **szanować prywatność dzieci i młodzieży** i informować je, gdy takie narzędzia są włączone,
- ▶ **działać na wszystkich urządzeniach i wersjach oprogramowania,**
- ▶ **współpracować z dostępnymi narzędziami kontroli rodzicielskiej**, takimi jak te dostępne w telefonach lub aplikacjach.



Narzędzia i metody kontroli rodzicielskiej mogą pomóc rodzinom w budowaniu **zaufania i wsparcia**, ale nigdy nie powinny prowadzić do inwigilacji ani pozbawiać dzieci ich praw. Nie powinny one także zastępować wbudowanych zabezpieczeń platformy.

Jesteś rodzicem lub opiekunem i szukasz wsparcia? W [portalu Lepszy internet dla dzieci](#) w sekcji Rodzice i opiekunowie dostępne są wskazówki, jak pomóc dzieciom w wykształceniu zdrowych nawyków cyfrowych i bezpiecznym poruszaniu się po wirtualnym świecie.

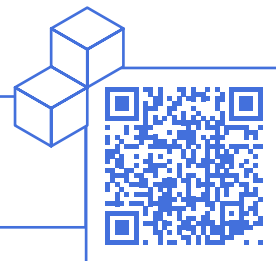


4. Kto dba o przestrzeganie przepisów aktu o usługach cyfrowych

Każdy kraj UE posiada **koordynatora ds. usług cyfrowych**, który współpracuje z Komisją Europejską w celu nadzorowania i monitorowania tego, w jaki sposób platformy wdrażają akt o usługach cyfrowych.



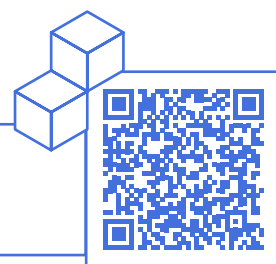
Zeskanuj kod QR, aby dowiedzieć się, kto jest koordynatorem ds. usług cyfrowych w Twoim kraju.



Każdy koordynator ds. usług cyfrowych może wyznaczyć organizacje, które specjalizują się w identyfikowaniu i zgłaszaniu nielegalnych i szkodliwych treści. Organizacje te nazywane są **zaufanymi podmiotami sygnalizującymi** (trusted flaggers). Gdy zgłaszają zastrzeżenia, platformy muszą podjąć szybkie działania. Organizacje te można porównać do sędziów sportowych, którzy egzekwują przepisy i zgłaszają wszelkie problemy i nadużycia, gdy tylko je zauważą.



Zeskanuj kod QR, aby dowiedzieć się, kto jest zaufanym podmiotem sygnalizującym w Twoim kraju.



5. Co dalej

Komisja Europejska i państwa członkowskie UE będą pilnować, aby platformy przestrzegały przepisów aktu o usługach cyfrowych i zapewniały dzieciom i młodzieży bezpieczeństwo w internecie. Komisja i państwa UE wspólnie:

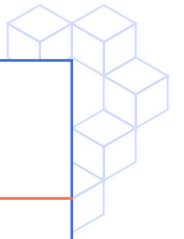
- ▶ kontrolują, czy platformy stosują się do wytycznych dotyczących ochrony małoletnich zawartych w akcie o usługach cyfrowych, a w przypadku ich nieprzestrzegania wszczynają postępowania prawne,
- ▶ testują i uruchamiają **unijną aplikację do weryfikacji wieku**,
- ▶ opracowują **unijny plan działania przeciwko cyberprzemocy**,
- ▶ analizują, jak **korzystanie z mediów społecznościowych wpływa na zdrowie psychiczne** dzieci i młodzieży.

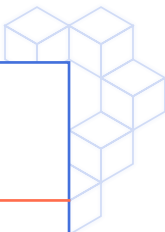
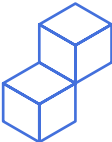


Cyfrowa pełnoletność

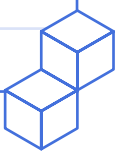
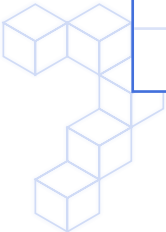
Wiek, w którym możesz zacząć samodzielnie korzystać z usług internetowych — bez konieczności uzyskania zgody rodziców. Zazwyczaj jest to 13 lub 18 lat, w zależności od przepisów w Twoim kraju i rodzaju usługi.

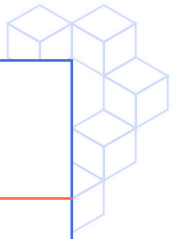






Twoje notatki





Gdzie znajdziesz więcej informacji i uzyskasz pomoc

Pełny tekst wytycznych aktu
o usługach cyfrowych dotyczących
ochrony małoletnich



Portal Lepszy internet dla dzieci
(Better Internet for Kids)



Niezależnie od tego, czy jesteś dzieckiem, nastolatkiem, rodzicem, opiekunem czy nauczycielem, możesz skontaktować się z centrum bezpieczniejszego internetu w Twoim kraju, aby otrzymać pomoc lub informacje dotyczące wszelkich kwestii związanych z internetem.



Zawsze możesz liczyć na pomoc – uzyskać wsparcie w **rozmowie telefonicznej, wysyłając maila lub na czacie internetowym**. Jest to **bezpłatne!**



Niniejsza broszura w prosty sposób wyjaśnia rodzinom wytyczne Komisji Europejskiej dotyczące ochrony nieletnich w ramach aktu o usługach cyfrowych. Pokazuje, jak platformy internetowe powinny dbać o bezpieczeństwo dzieci i młodzieży, stawiając ich prawa na pierwszym miejscu, uwzględniając prywatność i bezpieczeństwo na etapie projektowania usług, weryfikując wiek, zapewniając domyślne ustawienia prywatności, tworząc bezpieczne interfejsy, moderując szkodliwe treści, ułatwiając zgłaszanie i wspierając rodziców. Wszystko po to, aby młodzi użytkownicy mogli korzystać z internetu w wartościowy i bezpieczny sposób.



Komisja Europejska
Dyrekcja Generalna ds. Sieci
Komunikacyjnych, Treści i Technologii
Tekst ukończono w październiku 2025 r.

Niniejsza publikacja ma charakter wyłącznie informacyjny i nie jest dokumentem prawnym.
Luksemburg: Urząd Publikacji Unii Europejskiej, 2025
© Unia Europejska, 2025



Pobierz tę broszurę pod adresem:
<https://link.europa.eu/cgyKch>



Polityka Komisji w zakresie ponownego wykorzystywania jest realizowana na podstawie decyzji Komisji 2011/833/ UE z dnia 12 grudnia 2011 r. w sprawie ponownego wykorzystywania dokumentów Komisji (Dz.U. L 330 z 14.12.2011, s. 39, ELI: <http://data.europa.eu/eli/dec/2011/833/oj>). O ile nie wskazano inaczej, ponowne wykorzystywanie niniejszego dokumentu jest dozwolone na podstawie licencji Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>). Oznacza to, że ponowne wykorzystywanie jest dozwolone pod warunkiem odpowiedniego poinformowania o autorze oraz o wszelkich zmianach wprowadzonych w dokumencie.

PDF ISBN 978-92-68-31235-3 doi:10.2759/9560665 KK-01-25-130-PL-N
Print ISBN 978-92-68-31236-0 doi:10.2759/4991276 KK-01-25-130-PL-C