

Legal Alert

Lipiec 2026 r. | www.skslegal.pl

Nowe standardy ochrony dzieci w Internecie – co czeka dostawców platform cyfrowych?

Ponad dwa lata temu na terenie Unii Europejskiej zaczął obowiązywać Akt o usługach cyfrowych (DSA), stanowiący jeden z elementów długofalowej strategii zwiększania bezpieczeństwa dzieci w Internecie. Kolejnym krokiem w realizacji tej strategii była zapowiedź Ursuli von der Leyen, która we wrześniu 2025 r., w orędziu o stanie Unii, [ogłosiła](#) powołanie panelu ekspertów mającego wypracować praktyczne europejskie podejście do ochrony dzieci w sieci.

Raport o bezpieczeństwie dzieci w Internecie

13 lipca 2026 r. Ursula von der Leyen ogłosiła ukończenie przez specjalny panel Komisji Europejskiej ds. bezpieczeństwa dzieci w Internecie raportu, który rekomenduje m.in. unijne ograniczenie dostępu do mediów społecznościowych i innych usług cyfrowych dla dzieci poniżej 13 roku życia, stosowanie skutecznych metod weryfikacji wieku oraz rozszerzenie obowiązków dostawców w zakresie projektowania usług bezpiecznych dla małoletnich. Tym samym spodziewać należy się dalszych działań regulacyjnych obejmujących dostawców określanych obecnie szerokim pojęciem „social media+”.

Podmioty zobowiązane do weryfikacji wieku

Przewodnicząca KE nie wskazała konkretnej daty, od kiedy będą obowiązywały nowe regulacje dot. weryfikacji wieku ani jaka dokładnie grupa podmiotów zostanie nimi objęta. Z perspektywy zakładanego celu tj. zwiększenia bezpieczeństwa dzieci w Internecie, należy spodziewać się, że adresatami nowych obowiązków będą co najmniej dostawcy platform dostępnych dla dzieci (art. 28 DSA).

Natomiast dostawcy platform internetowych (np. social mediów, sklepów internetowych, internetowych platform handlowych) już teraz powinni ocenić, czy mogą podlegać nowym regulacjom przeprowadzając test trzech kroków.



Jeśli ich platforma jest dostępna dla małoletnich i może generować ryzyka dla dzieci warto już teraz ocenić jakie środki należy zastosować w celu ich skutecznego ograniczenia.

Test trzech kroków

– sprawdź gotowość swojej platformy

1. **Ocena profilu odbiorcy** platformy – weryfikacja czy platforma jest/może być kierowana do małoletnich;
2. **Ocena ryzyka** dla odbiorcy-dziecka – identyfikacja potencjalnego ryzyka związanego z korzystaniem z portalu na podstawie klasyfikacji 5-C (poniżej);
3. **Decyzja** dot. zastosowania odpowiednich środków bezpieczeństwa – ustalenie czy poziom ryzyka związany z korzystaniem z platformy jest na tyle wysoki, że małoletni nie powinni mieć do niej dostępu lub jak ograniczyć dostęp do ryzykownych funkcjonalności.

Klasyfikacja ryzyka 5-C

Organizacja Współpracy Gospodarczej i Rozwoju (OECD) przyjęła w 2021 r. nową [klasyfikację](#) ryzyka w środowisku cyfrowym, która była reakcją organizacji na znaczące zmiany w tym zakresie od 2011 r., kiedy sporządzona została ostatnia klasyfikacja.

Klasyfikacja ryzyka OECD pozwala dostawcom usług cyfrowych ocenić poziom i rodzaj ryzyka, które niosą ich platformy. Prawidłowe zidentyfikowanie ryzyka jest kluczowe dla dostosowania stron do ich nieletnich odbiorców i zastosowania adekwatnych środków bezpieczeństwa.

Raport sporządzony przez specjalny panel KE ds. bezpieczeństwa dzieci w Internecie, również powołuje się na tę klasyfikację, obrazując poszczególne zagrożenia powszechnie stosowanymi funkcjami na platformach internetowych, np. chatbot AI, reklama, komentarze.

OECD wyróżniło pięć rodzajów ryzyka:

Content Risks (ryzyka dot. treści) – ryzyka wynikające z czysto biernego uczestniczenia przez dziecko w środowisku cyfrowym, przejawiające się:

- treściami nienawiści – zdjęcia, słowa, gry obrażające dziecko w związku z posiadaną cechą;
- krzywdzącymi treściami – materiały nieadekwatne do wieku, np. pornografia;
- nielegalnymi treściami – materiały niedozwolone do publikacji nie tylko ze względu na wiek odbiorców, np. nagrania dot. aktu terroryzmu;
- dezinformacją - materiały wprowadzające w błąd, przedstawiające nieprawdziwe informacje.

Conduct Risks (ryzyka w związku z działaniem) – ryzyka wynikające z relacji użytkownik-użytkownik, gdzie dziecko stanowić może zagrożenie dla samego siebie w związku z własnym działaniem, np. wymiana erotycznych wiadomości (ang. „sexting”).

Contact Risks (ryzyka związane z kontaktem) – ryzyka wynikające z interakcji dziecka ze środowiskiem cyfrowym, gdzie dziecko jest bezpośrednią ofiarą działania osoby trzeciej.

Consumer Risks (ryzyka konsumenckie) – ryzyka wynikające z roli dziecka jako konsumenta gospodarki cyfrowej, przejawiające się:

- ryzykiem marketingowym – strategia marketingowa oddziałująca negatywnie na dzieci poprzez wykorzystanie ich naiwności, nieświadomości, np. influencer marketing;
- ryzykiem profilowania do celów komercyjnych – wykorzystywanie danych zamieszczanych przez dzieci w Internecie w celu jak najtrafniejszego dopasowania do dziecka treści mu przekazywanych, zachęcających go do danego działania, np. zakupu danego produktu;
- ryzykiem finansowym – podejmowanie nieświadomych decyzji finansowych przez dzieci bez wiedzy czy zgody opiekunów prawnych, np. zakup reklamowanego produktu;
- ryzykiem związanym z bezpieczeństwem – nieświadome wpadanie przez dzieci w pułapki Internetu, skutkujące pobraniem przez nie wirusa czy kradzieżą tożsamości dziecka.

Cross-cutting Risks (ryzyka przekrojowe) – ryzyka mogące wynikać ze wszystkich czynników wymienionych dla pozostałych ryzyk przez co mogą znacząco wpływać na dzieci, są to:

- ryzyko dot. prywatności – bezpośrednie i pośrednie dostarczanie dostawcom swoich danych przez dzieci;
- ryzyko związane z zastosowaniem zaawansowanej technologii – zbieranie danych w związku z korzystaniem ze sztucznej inteligencji, z urządzeń internetu rzeczy czy biometrii;
- ryzyko dla zdrowia i dobrostanu – narażenie na cyberprzemoc, krzywdzące treści etc.

Zapraszamy do kontaktu!



Agata Szeliga
Partner, radca prawny
☎ +48 698 660 648
✉ agata.szeliga@skslegal.pl



Alicja Maciążka
Prawnik
☎ +48 883 391 699
✉ alicja.maciazka@skslegal.pl