

DEPARTAMENTUL DE STUDII PARLAMENTARE ȘI POLITICI UE
DIRECȚIA STUDII ȘI DOCUMENTARE LEGISLATIVĂ

**BUNE PRACTICI PRIVIND
ACCESUL MINORILOR LA
PLATFORMELE DE SOCIAL
MEDIA ÎNTR-O SERIE DE STATE
MEMBRE ALE UNIUNII
EUROPENE**

studiu documentar

decembrie 2025

Lucrările elaborate în cadrul Direcției studii și documentare legislativă au caracter documentar și nu reprezintă punctul de vedere al Camerei Deputaților.

Documentele legislative oficiale au fost consultate în limba de origine, iar traducerea informațiilor relevante selectate nu reprezintă o traducere oficială, fiind furnizată ca un mijloc de înțelegere a unui document original, scris în altă limbă.

Baza de date cuprinzând totalitatea studiilor elaborate de Direcția studii și documentare legislativă poate fi accesată prin intermediul paginii de Intranet a Camerei Deputaților la adresa:
<http://www.cdep.ro/pls/dic/site2015.page?den=dsdl-home1>

Documentare și sinteză: Dan ALEXANDREANU
consilier parlamentar - Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

CUPRINS

SITUAȚIA EXISTENTĂ LA NIVELUL UNIUNII EUROPENE	4
ASPECTE COMPARATIVE	8
AUSTRIA.....	8
BELGIA	9
BULGARIA.....	10
CEHIA	11
CROAȚIA	13
DANEMARCA	14
ESTONIA.....	15
FINLANDA	16
FRANȚA.....	17
GERMANIA	18
IRLANDA	20
ITALIA	21
POLONIA	22
SLOVENIA	22
SPANIA	23
SUEDIA	24
ȚĂRILE DE JOS.....	25
UNGARIA.....	26
WEBOGRAFIE	27

SITUAȚIA EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

Bune practici privind accesul minorilor la platformele de social media

*Regulamentul privind serviciile digitale (DSA)*¹ al Uniunii Europene stabilește un cadru legal pentru a crește siguranța și responsabilitatea platformelor online, cu o atenție specială acordată protecției minorilor.

Bunele practici și orientările stabilite de Comisia Europeană, în special în contextul implementării DSA, vizează crearea unui mediu digital mai sigur pentru minori.

- *setări de confidențialitate implicite* - recomandarea este ca în momentul utilizării să fie personalizate setările de confidențialitate private.
- *sisteme de recomandare sigure* - platformele trebuie să utilizeze sisteme de recomandare mai sigure pentru a preveni expunerea minorilor la un conținut dăunător și la bucle care creează dependență (de exemplu, dezactivarea funcțiilor care stimulează implicarea, cum ar fi redarea automată sau alertele *push*).
- *restricții privind publicitatea direcționată* - este interzisă în mod absolut vizarea minorilor cu reclame bazate pe profilul lor, utilizând datele cu caracter personal.
- *instrumente de siguranță* - platformele trebuie să ofere instrumente mai puternice pentru blocarea, dezactivarea accesului și evitarea spamului de grup.
- *măsuri anti-exploatare* - sunt abordate recomandări precum interdicția de a descărca/captura de ecran a postărilor minorilor pentru a combate exploatarea sexuală.
- *termeni și condiții adaptate vârstei* - platformele trebuie să prezinte termeni și condiții prietenoși cu copiii, măsuri de siguranță bazate pe inteligență artificială și transparență în reclame.
- *limite privind tacticile manipulative de monetizare* - se impun restricții asupra schemelor care încurajează cheltuielile excesive (de exemplu, *loot box-uri*).

Modalități de verificare a vârstei

Verificarea eficientă a vârstei este o provocare majoră. Deși nu există o metodă unică obligatorie la nivel UE, se promovează abordări care să asigure protecția datelor.

- *auto-declararea* - este metoda cea mai comună, dar și cea mai ușor de eludat (de exemplu, introducerea unei date de naștere false).
- *Portofelul european de Identitate Digitală (EUDI Wallet)* - UE lucrează la implementarea acestui portofel (planificat până la sfârșitul anului 2026), care va permite utilizatorilor să își verifice vârsta către platforme fără a dezvălui alte informații personale.
- *prototipul tehnologic de verificare a vârstei (Age-verification blueprint)* Comisia Europeană a dezvoltat un prototip open-source, voluntar, care este compatibil cu viitorul EUDI Wallet.

¹ <https://eur-lex.europa.eu/RO/legal-content/summary/digital-services-act.html>

- *metode naționale*
Unele state membre (precum Franța, Italia, Spania) testează sau implementează deja soluții mai stricte, inclusiv aplicații de identitate digitală sau cerințe de prezentare a documentului de identitate pentru accesul la un conținut strict destinat adulților.
- *identitatea digitală* - este bazată pe instrumente oferite de stat pentru a verifica identitatea și vârsta.

Nivelul de responsabilitate al furnizorilor de servicii digitale

Regulamentul privind serviciile digitale analizează furnizorii de platforme online care sunt accesibile minorilor în centrul responsabilității.

- obligația generală de diligență

Toți furnizorii de platforme online accesibile minorilor trebuie să pună în aplicare măsuri adecvate și proporționale pentru a asigura un nivel ridicat de confidențialitate, siguranță și securitate pentru minori (art. 28 DSA).

- interzicerea publicității direcționate

Platformele nu au voie să utilizeze datele personale ale minorilor pentru publicitate direcționată atunci când cunosc cu o certitudine rezonabilă că utilizatorul este minor.

- evaluarea și reducerea riscurilor

Platformele online foarte mari (VLOP - *Very Large Online Platforms*) au obligații mai stricte, inclusiv efectuarea de evaluări anuale ale riscurilor sistemice pe care serviciile lor le prezintă pentru sănătatea fizică și mintală a minorilor și adoptarea de măsuri de atenuare a acestor riscuri.

- transparență

Platformele trebuie să fie transparente cu privire la algoritmii lor de recomandare și la modul în care sunt luate deciziile de moderare a conținutului.

- mecanisme de semnalare

Trebuie să se faciliteze utilizatorilor (inclusiv minorilor sau reprezentanților lor) posibilitatea de a semnala cu ușurință conținutul ilegal sau dăunător.

Regulamentul privind serviciile digitale² aplică o abordare bazată pe riscuri, impunând obligații diferite în funcție de mărimea și impactul platformei.

DSA clasifică furnizorii de servicii digitale în patru categorii principale, fiecare având un set progresiv de obligații:

categorie de serviciu	descriere	exemple de servicii	obligații cheie
Servicii de simplă transmitere (Conduit)	Transmiterea de date și furnizarea accesului la rețeaua de comunicații.	ISP-uri, rețele WiFi publice.	Fără răspundere pentru informațiile transmise, dacă nu sunt implicate activ.
Servicii de stocare în cache	Stocarea temporară automată a datelor pentru a îmbunătăți performanța.	Rețele de livrare de conținut (CDN).	Fără răspundere dacă respectă condițiile tehnice de acces.

² <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32022R2065>

categorie de serviciu	descriere	exemple de servicii	obligații cheie
Servicii de găzduire (Hosting)	Stocarea de informații furnizate de utilizatori.	Furnizori de <i>cloud</i> , servicii de găzduire web.	Obligația de a acționa prompt pentru a elimina conținutul ilegal de îndată ce iau cunoștință de el (<i>Notice and Action</i>).
Platforme online	Servicii de găzduire care diseminează informații către public (cea mai relevantă pentru social media).	Platforme social media, <i>marketplace</i> -uri, <i>app stores</i> .	Toate obligațiile de mai sus, plus mecanisme de raportare mai clare, transparența reclamelor și protecția minorilor.
VLOP și VLOSE	Platforme sau motoare de căutare online foarte mari (cu cel puțin 45 de milioane de utilizatori activi lunar în UE).	Facebook, TikTok, YouTube, Google Search.	Toate obligațiile de mai sus, plus obligații suplimentare de management al riscului.

Protecția minorilor

Art. 28 DSA impune platformelor online care sunt accesibile minorilor să ia măsuri pentru a asigura un nivel ridicat de confidențialitate, siguranță și securitate.

- interdicția publicității directe

Platformele online nu pot prezenta minorilor reclame bazate pe crearea de profiluri care utilizează date cu caracter personal (conform GDPR și DSA).

Cerința de "certitudine rezonabilă" se aplică atunci când platforma are o certitudine rezonabilă că utilizatorul este minor (de exemplu, dacă utilizatorul și-a declarat vârsta sau dacă vârsta a fost verificată).

- design și interfețe sigure

Interzicerea "*dark patterns*" presupune că platformele nu au voie să utilizeze interfețe care induc în eroare sau manipulează utilizatorii (inclusiv minori) pentru a lua decizii care nu sunt în interesul lor (de exemplu, tactici care fac complicată anularea unui abonament sau care forțează dezvăluirea de date).

Setările de confidențialitate implicite reprezintă acțiunea care trebuie realizată de platforme, respectiv implementarea celor mai ridicate standarde de confidențialitate și securitate pentru minori.

Obligații suplimentare pentru VLOP și VLOSE

Platformele online foarte mari (VLOP) și motoarele de căutare online foarte mari (VLOSE) au cele mai stricte obligații, menite să abordeze riscurile sistemice pe care le pot genera din cauza dimensiunii și impactului lor:

1. Evaluarea riscurilor sistemice

VLOP-urile trebuie să efectueze o evaluare anuală a riscurilor sistemice, inclusiv a celor legate de:

- răspândirea conținutului ilegal.
- impactul negativ asupra drepturilor fundamentale (respectiv libertatea de exprimare, protecția vieții private).

- impactul negativ asupra minorilor (sănătate fizică și mintală, exploatare, dependență).

2. Măsuri de atenuare a riscurilor

Pe baza evaluării, VLOP-urile trebuie să implementeze măsuri concrete de atenuare. Exemple relevante pentru minori:

- ajustarea sistemelor de recomandare pentru a preveni intrarea minorilor în "bule de conținut" sau expunerea la conținutul dăunător.
- audituri anuale independente pentru a verifica conformitatea cu DSA.
- punerea la dispoziția Comisiei Europene și a autorităților naționale a datelor (anonimizate) pentru monitorizarea riscurilor.

3. Transparența sistemelor de recomandare (art. 38)

VLOP-urile trebuie să ofere utilizatorilor posibilitatea de a modifica sau alege cel puțin un sistem de recomandare care nu se bazează pe profilul lor.

Nivelul de responsabilitate este susținut de un regim de sancțiuni sever. Neconformitatea cu DSA poate duce la amenzi de până la 6% din cifra de afaceri anuală a VLOP-ului.

Aplicarea DSA de către autoritățile naționale din UE

Aplicarea DSA se realizează printr-o combinație de acțiuni de supraveghere la nivel național și coordonare la nivelul UE, într-un sistem cunoscut sub numele de Mecanismul de Coordonare a Serviciilor Digitale.

1. Autoritățile de coordonare a serviciilor digitale (DSC)

Fiecare stat membru al UE este obligat să desemneze o autoritate națională principală care să acționeze în calitate de coordonator al serviciilor digitale (DSC - *Digital Services Coordinator*).

DSC este responsabil pentru aplicarea și punerea în executare a majorității obligațiilor din DSA pe teritoriul său, vizând furnizorii care își desfășoară activitatea în țara respectivă.

Statele membre pot fie să desemneze o autoritate existentă (de exemplu, autoritatea de reglementare în telecomunicații sau audiovizual, sau o autoritate specializată în protecția datelor), fie să creeze una nouă.

2. Competențele DSC

DSC-urile au atribuții largi pentru a asigura respectarea regulilor DSA, în special pentru platformele mai mici și medii.

- DSC-ul poate iniția investigații *ex officio* sau pe baza plângerilor utilizatorilor cu privire la presupusele încălcări ale DSA de către furnizorii care își desfășoară activitatea pe teritoriul său.

- Poate solicita furnizorului de servicii să implementeze măsuri corective sau să pună capăt imediat încălcării.

- DSC-ul poate impune sancțiuni financiare proporționale cu gravitatea încălcării. Legislația națională de transpunere a DSA stabilește nivelul acestor amenzi (care pot ajunge până la 6% din cifra de afaceri anuală pentru cele mai grave încălcări).

- DSC-urile sunt responsabile cu acreditarea organizațiilor sau persoanelor fizice care pot acționa ca "raportori de încredere" pentru notificarea conținutului ilegal.

3. Rolul suplimentar al Comisiei Europene

Deși DSC-urile gestionează majoritatea cazurilor, Comisia Europeană deține competențe directe de supraveghere și aplicare a legii în două situații critice:

- *supravegherea VLOP/VLOSE*

Comisia este singura responsabilă cu supravegherea și aplicarea DSA împotriva VLOP și a VLOSE. Deoarece impactul acestora depășește granițele naționale, Comisia aplică regulile direct și poate impune amenzi de până la 6% din cifra de afaceri globală.

- *mecanismul de coordonare*

Comisia supraveghează activitatea DSC-urilor și facilitează cooperarea dintre ele prin intermediul Comitetului European pentru Servicii Digitale, asigurând o aplicare uniformă a DSA în întreaga UE.

ASPECTE COMPARATIVE

AUSTRIA

Austria aplică un cadru dual - legislația UE direct aplicabilă (DSA, GDPR) și legislația națională complementară (*Audiovisuelle Mediendienste-Gesetz - AMD-G*³ și *DSA-Begleitgesetz*⁴).

Bune practici

Bunele practici din Austria sunt influențate de orientările DSA și de Strategia BIK+ (*Better Internet for Kids*)⁵ a UE:

- *design adecvat vârstei și control parental*

Legea federală privind serviciile media audiovizuale (*AMD-G*) impune furnizorilor de platforme de partajare video (VSP) să se asigure că întreg conținutul dăunător (în special cel care conține violență gratuită sau predominant acte sexuale nereflectate) este restricționat, de exemplu, prin utilizarea de sisteme de control parental.

- *vârsta digitală de consimțământ (GDPR)*

Austria a stabilit o vârstă digitală de consimțământ de 14 ani (sub prevederile Legii privind protecția datelor). Aceasta înseamnă că, pentru serviciile societății informaționale bazate pe consimțământ, copiii sub 14 ani au nevoie de autorizarea titularului responsabilității părintești.

- *verificarea obligatorie pentru conținutul extrem de dăunător*

AMD-G impune ca furnizorii de platforme de partajare video (VSP) să stabilească și să opereze sisteme de verificare a vârstei sau măsuri de control al accesului comparabile pentru a se asigura că minorii nu pot urmări în mod obișnuit cel mai dăunător conținut (pornografie nereflectată).

³ <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001412>

⁴ <https://www.parlament.gv.at/gegenstand/XXVII/I/2309>

⁵ <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52012DC0196>

- *utilizarea ID Austria*

Guvernul austriac promovează *ID Austria*, o formă de identitate digitală guvernamentală. Această infrastructură națională este văzută ca un mijloc potențial de a oferi o dovadă digitală a vârstei (*digital proof of age* - menționată în contextul ID Austria și al *eAusweise*), care ar permite verificarea vârstei fără a dezvălui platformei alte date de identificare (aliniindu-se cu viziunea EUDI Wallet).

- În prezent, platformele pentru adulți accesibile în Austria folosesc adesea auto-declararea vârstei, dar există o tendință de creștere a numărului de soluții avansate, bazate pe AI, pentru conformitate cu reglementările stricte.

Nivelul de responsabilitate al furnizorilor de servicii digitale

Responsabilitatea furnizorilor este definită de DSA și consolidată prin legislația națională de însoțire.

- *Autoritatea de reglementare (DSC)*

Autoritatea națională responsabilă cu aplicarea și supravegherea DSA în Austria este *KommAustria* (Autoritatea austriacă de Comunicații), care face parte din RTR.

- *Responsabilitatea legală pentru conținutul dăunător*

AMD-G impune platformelor de partajare video obligații suplimentare de a lua măsuri adecvate și proporționale împotriva conținutului care incită la infracțiuni (de exemplu, pornografia infantilă, incitarea la ură).

- *Raportori de încredere (Trusted Flaggers)*

Austria a desemnat mai multe entități naționale ca Raportori de încredere în baza DSA:

- *Rat auf Draht gemeinnützige GmbH* - acreditare pentru protecția minorilor și drepturile copilului.

- *ZARA - Zivilcourage und Antirassismusarbeit* - acreditare pentru violență cibernetică, discurs ilegal (de ură) și anti-discriminare.

BELGIA

Bune practici

Practicile din Belgia sunt aliniate cu cerințele DSA, cu un accent deosebit pe confidențialitate și design adecvat vârstei.

- *vârsta digitală de consimțământ*

Conform Legii belgiene privind protecția datelor, vârsta sub care copiii au nevoie de consimțământul parental pentru prelucrarea datelor lor personale pe platformele online este stabilită la 13 ani.

- *design prietenos pentru copii*

Platformele accesibile minorilor sunt încurajate să adopte principii de "*Privacy by Design*" și să folosească setări de confidențialitate stricte în mod implicit.

- *educație digitală*

Guvernul belgian (în special prin intermediul inițiativei *Better Internet for Kids* - *BIK* și organizațiile partenere) promovează activ alfabetizarea media și digitală în rândul tinerilor și părinților, considerată o barieră esențială împotriva riscurilor online.

În ceea ce privește modalitățile de verificare a vârstei, Belgia folosește metode care vizează echilibrul între eficacitate și respectarea principiului minimizării datelor din GDPR.

- *cardul de identitate electronic (eID)*

Belgia are un sistem dezvoltat de eID (Cardul de Identitate Electronic belgian) pentru cetățenii săi. Acesta poate servi, în viitor, ca bază pentru soluțiile de verificare a vârstei care se aliniază cu viitorul Portofel European de Identitate Digitală.

- *conținutul pornografic*

Există discuții și propuneri de legiferare pentru a impune metode de verificare a vârstei mai stricte pentru site-urile cu conținut pornografic, adesea bazate pe tehnologii terțe care oferă o dovadă a vârstei fără a dezvălui identitatea către site.

- *auto-declararea și consimțământul parental*

Pentru platformele de social media, metoda cea mai răspândită rămâne auto-declararea, susținută de cerința de a obține consimțământul parental pentru utilizatorii sub 13 ani, conform GDPR.

Nivelul de responsabilitate al furnizorilor de servicii digitale

Responsabilitatea furnizorilor este aplicată pe două niveluri principale, conform cadrului UE:

- *coordonatorul serviciilor digitale (DSC)*

În Belgia, funcția de coordonator al serviciilor digitale (DSC) este împărțită între mai multe autorități, reflectând structura federală a țării. Autoritatea Federală de Comunicații (BIPT) are un rol central.

- *responsabilitatea pentru conținutul ilegal*

Organizații precum *Child Focus* (centrul belgian pentru copii dispăruți și exploatați sexual) acționează ca raportori de încredere, notificând platformele cu privire la conținutul ilegal (în special materialul de abuz sexual asupra copiilor - CSAM). Platformele au obligația legală (sub DSA) de a acționa cu prioritate și rapiditate la aceste notificări.

BULGARIA

Bune practici

Bunele practici în Bulgaria sunt aliniate cu cerințele DSA, cu un accent deosebit pe educație și raportare.

- *vârsta digitală de consimțământ (GDPR)*

Bulgaria a stabilit vârsta sub care copiii au nevoie de consimțământul parental pentru prelucrarea datelor pe platformele online la 14 ani.

- *educație și campanii de conștientizare*

Bulgaria investește în campanii naționale pentru un internet mai sigur, promovând alfabetizarea media și informarea minorilor și a părinților cu privire la riscurile online (de exemplu, cyberbullying-ul, grooming-ul și dependența).

- *design axat pe copii*

Se dorește ca platformele să respecte obligațiile de diligență din DSA, asigurând setări de confidențialitate implicite sigure și evitând modelele întunecate care manipulează minorii.

În Bulgaria, la fel ca în majoritatea statelor membre, verificarea vârstei pentru platformele de social media se bazează pe auto-declarare, fiind în curs de dezvoltare soluții mai sigure și conforme cu confidențialitatea.

- auto-declararea vârstei

Pentru majoritatea platformelor, vârsta este stabilită pe baza informațiilor furnizate de utilizator. Platformele trebuie să solicite consimțământul parental pentru utilizatorii sub 14 ani.

- sisteme de verificare a vârstei pentru conținut restricționat

Pentru conținutul strict interzis minorilor, furnizorii trebuie să implementeze măsuri tehnice fiabile (precum sistemele de plată sau servicii terțe de verificare) pentru a restricționa accesul, dar implementarea acestora la nivel național este neuniformă.

Nivelul de responsabilitate al furnizorilor

Responsabilitatea furnizorilor de servicii digitale este stabilită de DSA și aplicată de autoritățile naționale.

- Coordonatorul serviciilor digitale

Autoritatea națională desemnată drept coordonator al serviciilor digitale (DSC) este Comisia pentru Reglementarea Comunicațiilor (CRC).

Aceasta este responsabilă cu supravegherea, punerea în aplicare și asigurarea respectării DSA de către furnizorii cu sediul în Bulgaria, inclusiv aplicarea obligațiilor de transparență, notificare și acțiune și, implicit, protecția minorilor.

- Responsabilitatea față de conținutul ilegal

Furnizorii (platformele) au obligația legală de a implementa un mecanism de semnalare ușor de utilizat și de a acționa prompt pentru a elimina conținutul ilegal de îndată ce iau cunoștință de acesta.

Organizații specializate, precum *Centrul național pentru un Internet Sigur*⁶ (parte a rețelei INSAFE/INHOPE), care activează și ca Hotline, pot fi desemnate ca Raportori de încredere. Platformele trebuie să acorde prioritate notificărilor primite de la aceste entități, sporindu-le responsabilitatea în combaterea conținutului dăunător sau ilegal, cum ar fi materialul de abuz sexual asupra copiilor.

CEHIA

Bune practici

Practicile din Republica Cehă se concentrează pe alinierea la cerințele DSA de protecție a minorilor și pe promovarea utilizării sigure a internetului.

- vârsta digitală de consimțământ

Legea cehă privind prelucrarea datelor cu caracter personal stabilește vârsta sub care copiii necesită consimțământul părinților pentru utilizarea serviciilor societății informaționale la 15 ani. Acesta este unul dintre pragurile mai înalte stabilite în UE, reflectând o abordare mai precaută.

- educație și prevenire

⁶ <https://www.safenet.bg/zabrana-na-soczialnite-mrezhi-za-decza-pod-15-godishna-vazrast/>

Există o atenție importantă pentru centrele de siguranță online și pentru inițiativele care promovează alfabetizarea media și securitatea cibernetică în școli, aceasta fiind o componentă cheie a strategiei naționale de protecție a minorilor.

- design-ul platformelor

Platformele accesibile minorilor sunt obligate să respecte obligațiile de diligență ale DSA, incluzând interdicția de a folosi datele personale ale minorilor pentru publicitate direcționată și obligația de a evita "modelele întunecate" care îi pot manipula.

În ceea ce privește modalitățile de verificare a vârstei, Cehia folosește o combinație de metode recunoscute la nivel european.

- auto-declararea cu consimțământ parental

Pentru majoritatea platformelor de social media, vârsta este verificată prin auto-declarare, dar platforma are obligația de a verifica consimțământul parental pentru utilizatorii sub 15 ani.

- verificarea strictă a vârstei pentru conținutul restricționat

Pentru conținutul care ar putea fi dăunător, furnizorii trebuie să folosească mecanisme eficiente de verificare a vârstei pentru a preveni accesul minorilor, deși soluțiile tehnice pot varia (de la sisteme bazate pe carduri de plată la soluții de identitate digitală terțe).

- identitatea digitală

Cehia are o infrastructură națională de identitate digitală (*e-Identita*), care se așteaptă să joace un rol crucial în integrarea cu viitorul Portofel European de Identitate Digitală (EUDI Wallet). Aceasta ar permite verificarea vârstei cu respectarea confidențialității.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este definit de DSA și aplicat de autoritățile cehice.

- coordonatorul serviciilor digitale

În Republica Cehă, autoritatea națională desemnată este Autoritatea Cehă pentru Telecomunicații (*ČTÚ*)⁷.

Această structură este responsabil cu supravegherea, aplicarea și asigurarea respectării DSA de către furnizorii de servicii digitale stabiliți în Cehia. Aceasta include aplicarea obligațiilor privind protecția minorilor și a mecanismului de notificare și acțiune.

- responsabilitatea față de conținutul ilegal

Furnizorii trebuie să pună la dispoziție instrumente ușoare pentru ca utilizatorii să raporteze conținutul ilegal și să acționeze prompt pentru a-l elimina sau dezactiva accesul.

În ceea ce privește raportorii de încredere, organizațiile specializate, cum ar fi *Safer Internet Center* și *Informační centrum pro prevenci a primární péči* (ICPP), se concentrează pe combaterea criminalității cibernetice și protecția minorilor.

⁷ <https://ctu.gov.cz/>

CROAȚIA

Bune practici

Bunele practici în Croația sunt guvernate de cerințele DSA de a asigura un nivel ridicat de siguranță, securitate și confidențialitate pentru minori.

- vârsta digitală de consimțământ

Legea croată privind protecția datelor personale stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 16 ani. Acesta este cel mai înalt prag permis de GDPR, reflectând o abordare strictă a protecției datelor minorilor.

- educație și resurse

Există un sprijin activ pentru "Centrul privind un Internet mai sigur", care oferă resurse, campanii de conștientizare și linii de asistență pentru copii și părinți privind riscurile online (de exemplu, cyberbullying sau grooming).

- obligații de design

Platformele trebuie să se conformeze cerințelor DSA de a evita modelele *dark patterns* și de a interzice publicitatea direcționată bazată pe profilarea minorilor.

Având o vârstă înaltă de consimțământ (16 ani), platformele care operează în Croația trebuie să fie deosebit de atente la verificarea vârstei și la obținerea consimțământului parental.

- auto-declararea și consimțământul părinților

Pentru majoritatea platformelor de social media, vârsta este stabilită prin auto-declarare, dar pentru utilizatorii sub 16 ani, platforma este obligată să depună eforturi rezonabile pentru a verifica consimțământul parental (deși metodele de verificare a consimțământului sunt adesea incomplete).

- cardul de identitate electronic

Croația dispune de un sistem național de identitate electronică, *e-Građani*⁸, care este utilizat pentru accesul securizat la serviciile publice. Această infrastructură va fi esențială pentru integrarea cu Portofelul european de Identitate Digitală, oferind în viitor o modalitate sigură și conformă cu GDPR de a verifica vârsta minorilor fără a dezvălui detalii de identificare.

- conținut restricționat

Pentru conținutul clasificat ca dăunător sau ilegal, furnizorii sunt obligați să implementeze măsuri tehnice eficiente de verificare a vârstei pentru a exclude prezența minorilor pe aceste site-uri.

Nivelul de responsabilitate al furnizorilor

- Coordonatorul serviciilor digitale

În Croația, autoritatea națională desemnată drept coordonator al serviciilor digitale este Consiliul pentru Media Electronică (*VEM - Vijeće za elektroničke medije*).

Această structură este responsabilă cu supravegherea și aplicarea DSA pentru furnizorii cu sediul în Croația. Rolul său include asigurarea respectării obligațiilor de transparență, a mecanismului de notificare și acțiune și a tuturor cerințelor specifice legate de protecția minorilor.

⁸ <https://gov.hr/>

- Responsabilitatea față de conținutul ilegal

Furnizorii (platformele) sunt obligați să ofere un instrument clar de raportare a conținutului ilegal și să acționeze prompt pentru eliminarea acestuia.

Raportorii de încredere sunt organizațiile croate cu expertiză în domeniul protecției minorilor și al drepturilor omului. Notificările acestora privind conținutul ilegal sau dăunător (precum materialul de abuz sexual asupra copiilor) trebuie tratate cu prioritate de către platforme, sporind responsabilitatea acestora.

DANEMARCA

Cadrul danez privind accesul minorilor la platformele de social media este influențat de legislația UE, dar este completat de o tradiție puternică de guvernare etică a datelor și de un accent pe drepturile copilului în mediul digital.

Bune practici

Danemarca pune un accent deosebit pe confidențialitate și responsabilitate socială corporativă din partea platformelor.

- vârsta digitală de consimțământ

Legea daneză privind protecția datelor⁹ stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 13 ani. Acesta este cel mai scăzut prag permis de GDPR, reflectând o încredere în capacitatea minorilor de a naviga în mediul digital de la o vârstă mai fragedă, cu sprijin.

- design axat pe confidențialitate

Se promovează adoptarea de către platforme a celor mai înalte standarde de confidențialitate (*Privacy by Design*). Autoritatea daneză pentru protecția datelor este foarte activă în a se asigura că platformele respectă drepturile copiilor, în special în ceea ce privește colectarea și utilizarea datelor.

- educație și resurse

Există un sprijin puternic pentru organizații care se concentrează pe siguranța online, cum ar fi *Red Barnet*, care oferă campanii și resurse ample pentru a crește alfabetizarea media și digitală a copiilor, precum și a părinților.

Danemarca, având o rată foarte mare de utilizare a soluțiilor de identitate digitală, se orientează către integrarea acestora cu cerințele de verificare a vârstei.

- identitatea digitală

Danemarca utilizează sistemul de identificare digitală *MitID* (care a înlocuit *NemID*). Deși *MitID* nu este folosit direct pentru a accesa platformele de social media, infrastructura guvernamentală de identitate este considerată baza pentru soluțiile viitoare de verificare a vârstei care vor folosi EUDI Wallet. Aceasta va permite verificarea vârstei cu respectarea principiului minimizării datelor.

- verificarea consimțământului

Având pragul de 13 ani, platformele sunt obligate să obțină consimțământul (sau să demonstreze că au făcut eforturi rezonabile în acest sens) de la părinți pentru utilizatorii mai tineri.

⁹ <https://www.retsinformation.dk/eli/lta/2018/502>

- *conținut restricționat*

Pentru conținutul ilegal sau dăunător, se impun măsuri tehnice fiabile de verificare a vârstei pentru a preveni accesul minorilor, în conformitate cu legislația UE și națională.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este definit de DSA și este aplicat de autoritățile daneze.

- *coordonatorul serviciilor digitale*

În Danemarca, autoritatea națională desemnată drept coordonator al serviciilor digitale este Autoritatea pentru concurență și consum (*KFST - Konkurrence- og Forbrugerstyrelsen*).

Aceasta este responsabilă cu supravegherea și asigurarea respectării DSA de către furnizorii cu sediul în Danemarca. Acest lucru include aplicarea obligațiilor de transparență, notificare și acțiune și a cerințelor de protecție a minorilor.

- *responsabilitatea față de conținutul ilegal*

Furnizorii au obligația legală de a oferi un mecanism clar de raportare a conținutului ilegal și de a acționa prompt pentru eliminarea acestuia.

Organizații precum *Red Barnet* joacă un rol activ în semnalarea conținutului periculos, inclusiv materialul de abuz sexual asupra copiilor și cyberbullying. Notificările din partea acestor entități trebuie tratate cu prioritate de către platforme.

ESTONIA

Bune practici

Estonia, fiind un lider recunoscut în digitalizarea serviciilor publice, încorporează practicile de protecție a minorilor în contextul său digital avansat.

- *vârsta digitală de consimțământ*

Legea estonă privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 13 ani.

- *educație digitală integrată*

Bunele practici includ integrarea alfabetizării media și a securității cibernetice în curriculumul școlar. *Centrul de securitate - cibernetică și pentru un Internet mai sigur* din Estonia (*Targalt internetis*¹⁰) joacă un rol activ în furnizarea de resurse pentru copii, părinți și profesori.

- *design axat pe utilizator și confidențialitate*

Platformele sunt obligate să respecte cerințele DSA de a asigura setări de confidențialitate implicite sigure pentru minori și de a interzice publicitatea direcționată bazată pe profilul ce rezultă din datelor minorilor.

Estonia are o infrastructură avansată de identitate digitală, care este esențială pentru a îndeplini cerințele DSA/GDPR de verificare a vârstei într-un mod prietenos cu confidențialitatea.

¹⁰ <https://www.targaltinternetis.ee/>

- identitatea digitală (eID / Smart-ID)

Estonia utilizează pe scară largă eID-ul său (prin cardul de identitate, Mobile-ID sau Smart-ID) pentru autentificarea securizată la serviciile online guvernamentale și private.

- verificarea vârstei bazată pe eID

Deși nu este obligatorie pentru *toate* platformele de social media, infrastructura eID oferă cel mai fiabil mecanism pentru platformele care necesită o verificare strictă a vârstei (de exemplu, conținutul pentru adulți), deoarece permite confirmarea autentică a vârstei utilizatorului fără a stoca date personale suplimentare la nivelul platformei.

- integrarea EUDI Wallet

Datorită experienței sale extinse în eID, Estonia va putea implementa rapid Portofelul european de Identitate Digitală, care va standardiza și mai mult verificarea vârstei cu respectarea confidențialității.

- verificarea consimțământului parental

Pentru utilizatorii sub 13 ani, platformele sunt obligate să obțină consimțământul verificabil al părinților sau al tutorilor legali.

Nivelul de responsabilitate al furnizorilor

În Estonia, coordonatorul serviciilor digitale este Autoritatea pentru Protecția Consumatorilor și Reglementare Tehnică (TTJA).

Aceasta este responsabilă cu supravegherea, aplicarea și asigurarea respectării DSA de către furnizorii cu sediul în Estonia, inclusiv aplicarea obligațiilor de transparență, notificare și acțiune și a cerințelor de protecție a minorilor.

- responsabilitatea față de conținutul ilegal

Furnizorii (platformele) trebuie să pună la dispoziție instrumente ușoare pentru ca utilizatorii să raporteze conținutul ilegal și să acționeze prompt pentru a-l elimina sau dezactiva accesul la aceste date.

FINLANDA

Bune practici

Finlanda, recunoscută pentru sistemul său educațional de calitate, integrează protecția minorilor în contextul digital prin accentul pus pe competențe și etică.

- vârsta digitală de consimțământ

Legea finlandeză privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 13 ani.

- educație media critică

Bunele practici se concentrează pe dezvoltarea gândirii critice și a alfabetizării media la elevi. *Centrul pentru Educația Media și Audiovizual* (KAVI) joacă un rol activ în furnizarea de materiale și cursuri pentru a-i ajuta pe tineri să evalueze critic informațiile și riscurile online.

- obligații DSA

Platformele trebuie să implementeze setări de confidențialitate implicite sigure pentru minori, să evite modelele *dark patterns* și să respecte interdicția publicității direcționate bazate pe profilul minorilor.

Finlanda se bazează pe infrastructura sa digitală avansată pentru soluții de verificare a vârstei care respectă confidențialitatea.

- identitatea digitală¹¹

Finlanda utilizează metode de autentificare electronică bazate pe sistemul bancar sau pe certificatele de identitate. Deși nu sunt folosite într-un mod universal de platformele de social media, această infrastructură securizată poate oferi o bază pentru servicii de verificare a vârstei sigure și conforme cu GDPR.

- integrarea EUDI Wallet

Infrastructura existentă va facilita integrarea cu EUDI Wallet, permițând minorilor să își confirme vârsta către platforme, fără a dezvălui informații personale de identificare.

- verificarea consimțământului parental

Pentru utilizatorii sub 13 ani, platformele sunt obligate să obțină consimțământul verificabil al părinților sau al tutorilor legali.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este definit de DSA și este aplicat de autoritatea națională desemnată. În Finlanda, aceasta este Autoritatea finlandeză de Transport și Comunicații (*Traficom*).

Organizații precum *Save the Children Finland* și *Centrul KAVI* (care administrează Hotline-ul național) pot fi desemnate ca Raportori de încredere. Notificările primite de la aceste entități, referitoare la conținutul dăunător sau ilegal (inclusiv CSAM), trebuie tratate cu prioritate.

FRANȚA

Bune practici

Franța a adoptat în iulie 2023 o lege care introduce o „majoritate digitală” și obligații suplimentare pentru platforme, depășind cerințele DSA în anumite privințe¹².

- vârsta legală digitală (*majorité numérique*)

Legea stabilește o vârstă digitală de 15 ani pentru înregistrarea și utilizarea rețelelor sociale. Furnizorii de servicii de rețele sociale care operează în Franța trebuie să refuze înregistrarea minorilor sub 15 ani fără autorizarea expresă a unuia dintre părinți.

- măsuri de siguranță implicite

La înregistrarea unui minor sub 15 ani (cu consimțământ parental), platformele sunt obligate să activeze un dispozitiv care să permită monitorizarea timpului petrecut și să informeze utilizatorii în mod regulat cu privire la durata utilizării.

Minorii și părinții lor trebuie să primească informații clare și adecvate cu privire la riscurile asociate activităților digitale și la condițiile de utilizare a datelor.

Franța este unul dintre cele mai avansate state în ceea ce privește impunerea unui standard tehnic specific pentru verificarea vârstei, concentrându-se pe respectarea confidențialității utilizatorilor (o cerință cheie a CNIL - Autoritatea de Protecție a Datelor).

¹¹ <https://www.suomi.fi/ohjeet-ja-tuki/tunnistus>

¹² <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>

- *Standardul național (Arcom)*

Autoritatea de Reglementare a Comunicațiilor Audiovizuale și Digitale (ARCOM) a elaborat un cadru de referință care impune ca soluțiile tehnice de verificare a vârstei să respecte principiul anonimității duble.

- *Principiul anonimității duble*

◦ *independență față de site* - Platforma (site-ul) nu trebuie să aibă acces la datele utilizate pentru verificarea vârstei (buletin, data nașterii).

◦ *confidențialitate față de verificator* - Furnizorul sistemului de verificare a vârstei nu trebuie să cunoască ce platformă accesează utilizatorul.

Practic, se testează sisteme care utilizează terți intermediari și criptografie avansată (*zero-knowledge proof*) pentru a returna doar o dovadă (de tipul "persoana are peste 15 ani") către platformă, fără a divulga identitatea utilizatorului către platformă sau istoricul navigării către terțul verificator.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este extrem de ridicat, fiind aplicat de autoritatea națională specializată. În Franța, aceasta este Autoritatea de Reglementare a Comunicațiilor Audiovizuale și Digitale (ARCOM).

ARCOM supraveghează aplicarea DSA, având competențe sporite, inclusiv impunerea obligațiilor specifice de verificare a vârstei și de luptă împotriva dezinformării. ARCOM cooperează strâns cu CNIL (Autoritatea de protecție a datelor) și cu Comisia Europeană.

Legea franceză prevede că, în cazul nerespectării obligației de a implementa o soluție tehnică de control al vârstei și de a obține consimțământul parental pentru minorii sub 15 ani, rețelele sociale pot primi o amendă de până la 1% din cifra de afaceri globală anuală (pe lângă amenzi de până la 6% prevăzute de DSA pentru alte încălcări). ARCOM are, de asemenea, competența de a solicita instanțelor blocarea accesului furnizat de ISP-uri către site-urile care nu implementează măsuri eficiente de verificare a vârstei pentru conținutul interzis minorilor.

Abordarea Franței este una dintre cele mai stricte din UE, punând un accent egal pe protecția efectivă a minorilor și pe respectarea confidențialității acestora prin soluții tehnice avansate.

GERMANIA

Germania are cel mai strict și mai complex cadru național din UE privind protecția minorilor în mediile online, bazat pe Legea de protecție a tinerilor¹³. Acest cadru completează și consolidează cerințele din Regulamentul privind Serviciile Digitale (DSA) și GDPR.

Bune practici

Cadrul german se concentrează pe clasificarea conținutului și pe obligarea furnizorilor de servicii să asigure un nivel ridicat de protecție împotriva conținutului dăunător.

¹³ <https://www.gesetze-im-internet.de/juschg/BJNR273000002.html>

- Legea de protecție a tinerilor clasifică conținutul online în două categorii principale de risc:

- conținut dăunător, care poate pune în pericol dezvoltarea minorilor (de exemplu, violență extremă, anumite forme de sexualitate explicită). Accesul la acesta trebuie restricționat strict prin verificarea eficientă a vârstei).
- conținut neadecvat, care poate fi nepotrivit pentru anumite grupe de vârstă (scene mai puțin violente, limbaj vulgar). Distribuția acestuia trebuie să fie asigurată doar la ore sau locuri potrivite (de exemplu, cu notificări clare de vârstă).

- Legea federală privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul parental pentru prelucrarea datelor pe platformele online la 16 ani. Acesta este cel mai înalt prag permis de GDPR.

- Platformele trebuie să implementeze măsuri tehnice și organizaționale pentru a se asigura că minorii sunt protejați de conținutul periculos. Acestea includ setări de confidențialitate implicite sigure și măsuri pentru limitarea riscurilor legate de contactul cu străinii.

Germania impune standarde foarte exigente pentru verificarea vârstei în cazul conținutului clasificat ca fiind dăunător.

- *sisteme de verificare*

Platformele care oferă conținut dăunător sau restricționat de vârstă trebuie să utilizeze sisteme de verificare a vârstei (*Age Verification Systems - AVS*) care sunt recunoscute și certificate ca fiind eficiente de către autoritatea de reglementare (KJM).

Metodele acceptate trebuie să asigure că minorul nu poate eluda sistemul și pot include soluții bazate pe:

- identificare prin buletin sau alte documente oficiale (cu păstrarea confidențialității).
- coduri PIN obținute prin sisteme de plată sigure sau prin poștă.
- soluții criptografice avansate, care se află în etapa de dezvoltare.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este extrem de ridicat, supravegheat de o autoritate specializată în media și protecția minorilor.

- *Comisia pentru protecția minorilor în media (KJM - Kommission für Jugendmedienschutz)* este autoritatea responsabilă cu aplicarea prevederilor legale și cu supravegherea măsurilor de protecție a minorilor pe platforme. KJM are competența de a clasifica conținutul și de a impune platformelor să implementeze sisteme eficiente de verificare a vârstei.

- *Coordonatorul serviciilor digitale (DSC)*

Funcția de DSC este împărțită între mai multe autorități, Autoritatea federală a rețelelor jucând un rol central în aplicarea DSA pentru platformele online (alături de autoritățile de protecție a minorilor de la nivel de land).

IRLANDA

Cadrul legal din Irlanda privind accesul minorilor la platformele de social media are o importanță deosebită, deoarece Irlanda este țara de stabilire (și, prin urmare, principalul regulator) pentru majoritatea marilor companii de tehnologie din UE (Meta, Google, TikTok, X, etc.). Astfel, modul în care Irlanda aplică DSA și GDPR are un impact paneuropean.

Bune practici

Practicile din Irlanda sunt puternic axate pe aplicarea strictă a normelor de confidențialitate și a obligațiilor DSA, dat fiind rolul său de hub tehnologic.

- vârsta digitală de consimțământ

Legea irlandeză stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 16 ani.

- supravegherea protecției datelor (DPC)

Autoritatea irlandeză de Protecție a Datelor a fost extrem de activă în investigarea modului în care marile platforme (VLOP-uri) gestionează datele minorilor, impunând amenzi semnificative pentru încălcarea GDPR (de exemplu, împotriva Meta/Instagram).

- design axat pe confidențialitate

Platformele sunt obligate să implementeze setări de confidențialitate implicite sigure pentru minori și să interzică publicitatea direcționată bazată pe datele minorilor.

Datorită pragului înalt de consimțământ (16 ani) și a supravegherii stricte din partea DPC, platformele stabilite în Irlanda sunt sub o presiune constantă de a găsi metode de verificare a vârstei care să fie eficiente și să respecte confidențialitatea.

- verificarea consimțământului parental

Pentru utilizatorii sub 16 ani, platformele sunt obligate să depună eforturi rezonabile pentru a verifica consimțământul parental în conformitate cu prevederile GDPR.

Marile platforme experimentează cu sisteme terțe (bazate pe AI sau pe verificarea documentelor de identitate) o serie de metode pentru a îndeplini standardul de diligență. Aceste soluții trebuie să fie aprobate de DPC în ceea ce privește conformitatea cu GDPR.

Nivelul de responsabilitate al furnizorilor

În Irlanda, autoritatea națională desemnată drept DSC este Comisia pentru Comunicații. Aceasta este responsabilă cu supravegherea, aplicarea și asigurarea respectării DSA de către furnizorii din Irlanda. Aceasta include aplicarea obligațiilor de transparență, notificare și acțiune și a cerințelor specifice legate de protecția minorilor.

- Organizații irlandeze precum *Hotline Ireland* joacă un rol vital în semnalarea conținutului ilegal. Platformele trebuie să acorde prioritate notificărilor primite de la aceste entități.

- Atât Comisia pentru Comunicații, cât și DPC (pentru GDPR) au competența de a impune sancțiuni importante. Amenda maximă pentru încălcarea DSA este de 6% din cifra de afaceri globală anuală, iar pentru încălcările GDPR (aplicate de DPC) poate ajunge la 4% din cifra de afaceri globală anuală.

ITALIA

Bune practici

Italia a pus un accent puternic pe combaterea tulburărilor de comportament și a dependenței de platforme, vizând, de asemenea, protecția imaginii minorilor.

- *vârsta digitală de consimțământ*

Legea italiană privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 14 ani.

- *prevederi anti-cyberbullying (Legea 71/2017)¹⁴*

Italia are o lege națională specifică pentru combaterea *cyberbullying*-ului, care oferă minorilor, chiar și fără implicarea părinților, posibilitatea de a solicita platformelor și furnizorilor de servicii ștergerea sau blocarea conținutului defăimător sau dăunător.

- *accent pe sănătate și dependență*

Autoritățile italiene au intervenit activ, solicitând platformelor să implementeze măsuri mai stricte de verificare a vârstei și de protecție a datelor pentru a preveni accesul copiilor sub vârsta legală și pentru a limita riscul de dependență.

Conform DSA, este interzisă publicitatea direcționată bazată pe profilul minorilor. În plus, autoritățile italiene au monitorizat strict campaniile publicitare care vizează minorii, în special cele legate de jocurile de noroc sau de produse care pot afecta sănătatea.

Italia a avut o abordare proactivă în impunerea verificării vârstei, solicitând platformelor să fie mai diligente.

- Autoritatea italiană pentru protecția datelor a impus platformelor să își revizuiască și să își îmbunătățească sistemele de verificare a vârstei, considerând auto-declararea ca fiind insuficientă pentru a respecta cerințele GDPR privind vârsta de 14 ani.

- Italia utilizează pe scară largă sistemul SPID (*Sistema Pubblico di Identità Digitale*) pentru accesul la serviciile guvernamentale. Această infrastructură națională reprezintă baza pentru integrarea cu viitorul EUDI Wallet. SPID-ul permite o verificare a vârstei securizată și conformă cu GDPR, esențială pentru a îndeplini standardul de "efort rezonabil" al platformelor.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este stabilit de DSA și este aplicat de autoritățile naționale specializate.

În Italia, autoritatea națională desemnată drept Coordonator al serviciilor digitale (DSC) este Autoritatea pentru Comunicații (*AGCOM - Autorità per le Garanzie nelle Comunicazioni*).

AGCOM este responsabilă cu supravegherea și asigurarea respectării DSA de către furnizorii stabiliți în Italia, inclusiv aplicarea obligațiilor de transparență, Notificare și Acțiune și a cerințelor specifice legate de protecția minorilor (Art. 28).

Deși AGCOM este DSC-ul, Autoritatea de Protecție a Datelor menține o putere semnificativă de supraveghere, în special asupra modului în care platformele prelucrează datele minorilor (respectarea vârstei de 14 ani și a consimțământului parental). GPDP a inițiat investigații și a impus sancțiuni platformelor pentru nerespectarea acestor norme.

¹⁴ <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017-05-29;71>

POLONIA

Bune practici

Polonia se aliniază cerințelor DSA, cu un accent aparte pe etica socială și protecția datelor personale.

- vârsta digitală de consimțământ

Legea poloneză privind protecția datelor cu caracter personal stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 16 ani.

Bunele practici includ un sprijin important pentru Centrul de Siguranță privind Internet-ul din Polonia, care desfășoară campanii extinse de conștientizare, alocând resurse educaționale și linii de asistență pentru minori, părinți și profesori.

Având un prag înalt de consimțământ, platformele care operează în Polonia trebuie să fie diligente în verificarea vârstei și a consimțământului parental.

- verificarea consimțământului parental

Pentru utilizatorii sub 16 ani, platformele sunt obligate să obțină consimțământul verificabil al părinților sau al tutorilor legali, ceea ce necesită adesea soluții tehnice deosebite.

- sistemul de identitate digitală (eID)

Polonia utilizează un sistem național de identitate electronică, care va fi esențial pentru integrarea cu viitorul Portofel European de Identitate Digitală.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este stabilit de DSA și este aplicat de autoritatea națională desemnată. Aceasta este Autoritatea de Reglementare a Telecomunicațiilor și a Poștei (*UKE - Urząd Komunikacji Elektroniczej*).

UKE este responsabilă cu supravegherea, aplicarea și asigurarea respectării DSA de către furnizorii cu sediul în Polonia. Aceasta include aplicarea obligațiilor de transparență, notificare și acțiune și a cerințelor specifice legate de protecția minorilor.

Furnizorii (platformele) au obligația legală de a oferi un mecanism clar de raportare a conținutului ilegal și de a acționa prompt pentru eliminarea acestuia.

- Organizații specializate, precum Centrul Național de Contact¹⁵, care luptă împotriva conținutului dăunător și ilegal, pot fi desemnate ca raportori de încredere.

SLOVENIA

Bune practici

Slovenia se aliniază cerințelor DSA, punând accent pe dreptul la informare și pe un mediu digital sigur.

- vârsta digitală de consimțământ

Legea slovenă privind protecția datelor personale stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 15 ani.

¹⁵ <https://www.saferinternet.pl/>

- Există un sprijin activ pentru Centrul pentru un Internet mai sigur (*Safe.si*), care oferă resurse extinse, linii de asistență și campanii de conștientizare pentru a sprijini minorii și părinții în gestionarea riscurilor online.

Platformele sunt obligate să implementeze setări de confidențialitate implicite sigure pentru minori, să evite modelele *dark patterns* și să respecte interdicția publicității direcționate.

Datorită pragului de consimțământ de 15 ani, platformele care operează în Slovenia sunt obligate să fie diligente în verificarea vârstei și a consimțământului parental.

- *verificarea consimțământului parental*

Pentru utilizatorii sub 15 ani, platformele trebuie să depună eforturi rezonabile pentru a verifica consimțământul parental în conformitate cu GDPR.

- *identitatea digitală (SI-PASS)*¹⁶

Slovenia utilizează un sistem național de identificare electronică, *SI-PASS*, pentru accesul securizat la serviciile publice. Această infrastructură este esențială pentru integrarea cu viitorul Portofel European de Identitate Digitală.

- *conținut restricționat*

Pentru conținutul strict interzis minorilor, furnizorii sunt obligați să implementeze măsuri tehnice eficiente de verificare a vârstei pentru a exclude prezența minorilor.

Nivelul de responsabilitate al furnizorilor

În Slovenia, autoritatea națională desemnată drept coordonator al serviciilor digitale este Autoritatea de Reglementare a Telecomunicațiilor și Poștei (*AKOS*).

AKOS este responsabilă cu supravegherea, aplicarea și asigurarea respectării *DSA* de către furnizorii cu sediul în Slovenia.

SPANIA

Spania a adoptat o poziție foarte strictă în ceea ce privește protecția minorilor în mediul digital, nu doar transpunând legislația UE (*DSA* și *GDPR*), regiunile autonome adoptând o serie de legi care abordează dependența, abuzul sexual asupra copiilor și utilizarea etică a datelor.

Bune practici

Spania a consolidat protecția minorilor prin Legea organică nr. 8/2021 privind protecția integrală a copiilor și adolescenților împotriva violenței¹⁷ și prin directivele autorităților sale de reglementare.

- *vârsta digitală de consimțământ*

Legea spaniolă privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 14 ani.

- *protecția împotriva violenței online*

¹⁶ <https://www.si-trust.gov.si/en/si-pass>

¹⁷ <https://www.boe.es/boe/dias/2021/06/05/pdfs/BOE-A-2021-9347.pdf>

Legea 8/2021 impune platformelor și școlilor obligații specifice de a identifica și de a raporta cazurile de violență și abuz online, punând un accent deosebit pe răspunderea instituțiilor de a acționa proactiv.

- *evaluarea riscurilor*

Platformele online sunt supuse cerințelor DSA de a realiza evaluări de risc periodice și de a implementa măsuri de atenuare, în special pentru riscurile sistemice care afectează minorii.

Spania a fost una dintre primele țări din UE care a solicitat în mod explicit platformelor să implementeze sisteme de verificare a vârstei pentru a se asigura că minorii nu accesează conținut neadecvat.

- *soluții de identitate digitală*

Spania utilizează un sistem avansat de identitate digitală (*CI@ve*, *MiDNI*). Aceste soluții oferă o infrastructură națională viabilă pentru integrarea cu viitorul *EUDI Wallet*.

Aceste soluții digitale sunt considerate mijloace sigure și conforme cu GDPR pentru a dovedi vârsta pe platforme, fără a dezvălui date de identificare complete, respectând principiul minimizării datelor.

- Autoritatea spaniolă pentru Protecția Datelor (AEPD) a fost foarte strictă în a solicita platformelor să își îmbunătățească sistemele de verificare a vârstei pentru a îndeplini standardul de "efort rezonabil" (GDPR), considerând auto-declararea ca fiind insuficientă pentru a valida consimțământul minorilor.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este stabilit de DSA și este aplicat de autoritățile naționale specializate.

În Spania, autoritatea națională desemnată drept coordonator al serviciilor digitale este Secretariatul de Stat pentru Digitalizare și Inteligență Artificială (*SEDIA*).

Această structură deține o capacitate semnificativă de supraveghere, investigând modul în care platformele prelucrează datele minorilor, inițiind investigații împotriva platformelor care nu au reușit să verifice consimțământul minorilor sub 14 ani.

Organizații spaniole precum *Protege Tu Pantalla* și *Internet Segura for Kids (IS4K)* joacă un rol activ în semnalarea conținutului periculos și abuziv.

SUEDIA

Cadrul suedez pentru accesul minorilor la platformele de social media este definit de legislația UE, fiind completat de o tradiție națională puternică axată pe inovație, transparență și drepturile copilului.

Bune practici

Suedia promovează un mediu digital deschis, dar sigur, punând accent pe educație și conformitatea cu cele mai înalte standarde de confidențialitate.

- *vârsta digitală de consimțământ*

Legea suedeză privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 13 ani.

- se acordă un sprijin important pentru inițiativele care promovează alfabetizarea media și digitală critică. Consiliul pentru Media joacă un rol central în monitorizarea mediului online și în furnizarea de resurse educaționale pentru a-i ajuta pe tineri să gestioneze riscurile.

Suedia se bazează pe infrastructura sa digitală avansată pentru soluții de verificare a vârstei, asigurând în același timp respectarea confidențialității.

- *identitatea bancară electronică (BankID)*

Suedia utilizează pe scară largă BankID, un sistem de identificare electronică bazat pe activitatea bancară, pentru accesul securizat la servicii online.

- *verificarea vârstei*

Deși nu este obligatoriu pentru toate platformele de social media, infrastructura BankID (sau soluțiile similare) este utilizată ca model pentru serviciile de verificare a vârstei sigure și conforme cu GDPR, în special pentru conținutul restricționat.

- *verificarea consimțământului parental*

Pentru utilizatorii sub 13 ani, platformele sunt obligate să obțină consimțământul verificabil al părinților sau al tutorilor legali.

Nivelul de responsabilitate al furnizorilor

Nivelul de responsabilitate este stabilit de DSA și este aplicat de autoritatea națională desemnată, cu accent pe transparență.

În Suedia, autoritatea națională desemnată drept coordonator al serviciilor digitale este Autoritatea suedeză pentru Poștă și Telecomunicații¹⁸ (*PTS - Post- och telestyrelsen*).

Furnizorii au obligația de a oferi un mecanism clar de raportare a conținutului ilegal și de a acționa prompt pentru eliminarea acestuia.

Organizații specializate, precum *Safer Internet Centre*, care operează o linie de urgență, pot fi desemnate ca raportori de încredere.

ȚĂRILE DE JOS

Cadrul legal din Țările de Jos privind accesul minorilor la platformele de social media este definit de legislația UE, fiind completat de o abordare națională axată pe autonomia minorilor și supravegherea strictă a prelucrării datelor.

Bune practici

Țările de Jos s-au aliniat cerințelor DSA, punând un accent deosebit pe educație și pe dreptul minorilor la confidențialitate și la dezvoltare personală.

- *vârsta digitală de consimțământ*

Legea olandeză privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 16 ani. Acesta este cel mai înalt prag permis de GDPR, reflectând o abordare strictă a confidențialității minorilor.

- *educație și resurse*

¹⁸ <https://pts.se/>

Există un sprijin important pentru Consiliul pentru Media (*Mediawijzer*), care oferă resurse ample și campanii pentru a promova alfabetizarea media și utilizarea responsabilă a internetului de către tineri.

Având un prag înalt de consimțământ (16 ani), platformele care operează în Țările de Jos sunt obligate să fie deosebit de diligente.

- *verificarea consimțământului parental*

Pentru utilizatorii sub 16 ani, platformele sunt obligate să depună eforturi rezonabile pentru a verifica consimțământul parental în conformitate cu GDPR. Autoritatea de Protecție a Datelor (*Autoriteit Persoonsgegevens - AP*) supraveghează strict conformitatea cu prevederile legale.

- *identitatea digitală (DigiD)*

Țările de Jos utilizează un sistem național de identificare digitală (*DigiD*) pentru accesul la serviciile guvernamentale.

- EUDI Wallet este considerat soluția pe termen lung pentru a permite platformelor să verifice vârsta într-un mod care respectă principiul minimizării datelor (furnizând doar dovada că utilizatorul are peste 16 ani, fără a dezvălui identitatea completă).

Nivelul de responsabilitate al furnizorilor

- În Țările de Jos, autoritatea națională desemnată drept coordonator al serviciilor digitale (DSC) este Autoritatea pentru Consumatori și Piață (*ACM - Autoriteit Consument en Markt*).

- Autoritatea pentru protecția datelor deține o putere semnificativă de supraveghere, în special asupra modului în care platformele prelucrează datele minorilor.

- Raportori de încredere sunt organizații specializate, precum *Meldpunt Internet Discriminatie (Meldpunt)* și *Centrul pentru Conținut Illegal pe Internet (IVR)*, care joacă un rol activ în semnalarea conținutului dăunător și ilegal.

UNGARIA

Cadrul legal din Ungaria privind accesul minorilor la platformele de social media este definit de legislația UE, fiind completat de o legislație națională care pune un accent puternic pe protecția morală a minorilor și pe intervenția guvernamentală în mediul online.

Bune practici

- *vârsta digitală de consimțământ*

Legea ungară privind protecția datelor stabilește vârsta sub care copiii necesită consimțământul părinților pentru prelucrarea datelor pe platformele online la 16 ani.

- Legislația ungară, în special cea care vizează media, include prevederi stricte privind conținutul considerat dăunător moral sau neadecvat pentru minori¹⁹. Deși aceste prevederi sunt aplicate în principal mediilor tradiționale, există o presiune tot mai mare ca platformele online să respecte standarde similare de protecție morală.

¹⁹ <https://mkogy.jogtar.hu/jogszabaly?docid=A2400030.TV>

Datorită pragului înalt de consimțământ (16 ani), platformele care operează în Ungaria sunt obligate să gestioneze cu atenție verificarea vârstei și a consimțământului parental.

- *verificarea consimțământului parental*

Pentru utilizatorii sub 16 ani, platformele sunt obligate să depună eforturi rezonabile pentru a verifica consimțământul parental în conformitate cu prevederile GDPR.

- *sisteme de identitate electronică*

Ungaria utilizează un sistem național de identitate electronică, care va fi relevant pentru integrarea cu viitorul Portofel European de Identitate Digitală.

Nivelul de responsabilitate al furnizorilor

În Ungaria, autoritatea națională desemnată drept coordonator al serviciilor digitale este Autoritatea națională pentru Media și Comunicații (NMHH - *Nemzeti Média- és Hírközlési Hatóság*).

Autoritatea națională pentru Protecția Datelor și Libertatea de Informare (NAIH) deține o putere semnificativă de supraveghere, în special asupra modului în care platformele prelucrează datele minorilor, asigurând respectarea pragului de consimțământ de 16 ani.

WEBOGRAFIE

- <https://eur-lex.europa.eu/RO/legal-content/summary/digital-services-act.html>
- <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32022R2065>
- <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001412>
- <https://www.parlament.gv.at/gegenstand/XXVII/I/2309>
- <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52012DC0196>
- <https://www.safenet.bg/zabrana-na-soczialnite-mrezhi-za-decza-pod-15-godishna-vazrast/>
- <https://ctu.gov.cz/>
- <https://gov.hr/>
- <https://www.retsinformation.dk/eli/lta/2018/502>
- <https://www.targaltinternetis.ee/>

- <https://www.suomi.fi/ohjeet-ja-tuki/tunnistus>
- <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>
- <https://www.gesetze-im-internet.de/juschg/BJNR273000002.html>
- <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017-05-29;71>
- <https://www.saferinternet.pl/>
- <https://www.si-trust.gov.si/en/si-pass>
- <https://www.boe.es/boe/dias/2021/06/05/pdfs/BOE-A-2021-9347.pdf>
- <https://pts.se/>
- <https://mkogy.jogtar.hu/jogszabaly?docid=A2400030.TV>