Declarație

Declarația 1/2025 privind asigurarea vârstei

Adoptată la 11 februarie 2025[1]

Comitetul European pentru Protecția Datelor adoptă următoarea declarație:

1. CONTEXTUL ȘI SCOPUL PREZENTEI DECLARAȚII

1. Cadrul european de reglementare solicită o protecție sporită a copiilor în mediul digital. De exemplu, Directiva serviciilor mass-media audiovizuale[2], pe care statele membre au transpus-o în legislația lor națională, subliniază posibilitatea de a pune în aplicare măsuri de verificare a vârstei (articolele 6a și 28b), RGPD introduce cerințe privind vârsta minimă pentru consimțământul pentru prelucrarea datelor cu caracter personal în contextul serviciilor societății informaționale (articolul 8), Regulamentul privind o piață unică pentru serviciile digitale[3] menționează verificarea vârstei ca măsură de atenuare a riscurilor [articolul 35 alineatul (1)], iar o serie de state membre au introdus în legislația lor națională cerințe privind vârsta minimă pentru încheierea de acte juridice, exercitarea anumitor drepturi sau accesul la anumite bunuri și servicii.

2. În plus, diferite inițiative naționale și europene, cum ar fi „Un internet mai bun pentru copii” (BIK+), identifică asigurarea vârstei ca fiind o soluție pentru îmbunătățirea bunăstării online a copiilor printr-un mediu digital sigur și adaptat vârstei, în conformitate cu drepturile și principiile digitale europene[4].

[1] La 24 februarie 2025, s-au efectuat rectificări minore ale formatării prezentului document. Alte rectificări minore au fost aduse, la 1 aprilie 2025, la punctul 16 și la punctul 22 litera (b).

[2] Directiva (UE) 2018/1808 a Parlamentului European și a Consiliului din 14 noiembrie 2018 de modificare a Directivei 2010/13/UE privind coordonarea anumitor dispoziții stabilite prin acte cu putere de lege sau acte administrative în cadrul statelor membre cu privire la furnizarea de servicii mass-media audiovizuale (Directiva serviciilor mass-media audiovizuale) având în vedere evoluția realităților pieței, https://eur-lex.europa.eu/eli/dir/2018/1808/oj.

[3] Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale), https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

[4] *Better Internet for Kids, Guide to age assurance*, (Un internet mai bun pentru copii, Ghid privind asigurarea vârstei) https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest.

3. Pe baza definiției furnizate în raportul de cercetare intitulat *„Mapping age assurance typologies and requirements”*[5] (Cartografierea tipologiilor și a cerințelor asigurării vârstei), în cadrul prezentului document expresia „asigurarea vârstei” se va utiliza ca *„termen generic pentru metodele utilizate pentru a determina vârsta sau intervalul de vârstă al unei persoane cu niveluri diferite de încredere sau certitudine*”. Același raport menționează trei categorii principale ale asigurării vârstei: estimarea vârstei, verificarea vârstei și declarația pe proprie răspundere.
4. Asigurarea vârstei prezintă riscuri specifice în ceea ce privește protecția datelor, având potențialul de a avea un impact negativ nu numai asupra dreptului persoanelor fizice la protecția datelor lor cu caracter personal, ci și asupra altor drepturi și libertăți[6], cum ar fi dreptul la nediscriminare, dreptul la integritate al persoanei, dreptul la libertate și securitate și dreptul la liberă exprimare și informare.

5. Recunoscând importanța unei abordări coerente la nivelul UE pe tema asigurării vârstei, CEPD dorește să ofere orientări specifice și principii de nivel înalt care decurg din RGPD și care ar trebui luate în considerare atunci când datele cu caracter personal sunt prelucrate în contextul asigurării vârstei.

6. Principiile propuse urmăresc reconcilierea protecției copiilor cu protecția datelor cu caracter personal în contextul asigurării vârstei.

7. S-a acordat prioritate abordării cerințelor privind principiile de bază prevăzute la articolul 5 din RGPD (legalitate, echitate și transparență, limitări legate de scop, reducerea la minimum a datelor, exactitate, limitări legate de stocare, confidențialitate, integritate și responsabilitate) și asigurării faptului că aceste principii de protecție a datelor sunt puse în aplicare în mod corespunzător și rămân solide în timp, astfel cum se prevede la articolul 25 din RGPD „Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit” și la articolul 32 din RGPD „Securitatea prelucrării”.

8. Prezenta declarație se axează pe principiile aplicabile diferitelor cazuri de utilizare online, inclusiv atunci când o vârstă minimă este prevăzută prin lege sau în alt mod pentru achiziționarea de produse, pentru utilizarea de servicii care îi pot afecta pe copii sau pentru încheierea de acte juridice, precum și atunci când există obligația de a-i proteja pe copii (de exemplu, pentru a se asigura că serviciile sunt concepute sau oferite într-un mod adecvat vârstei).

9. CEPD poate lua în considerare, de asemenea, emiterea – ori de câte ori este relevant și în alte documente – de orientări suplimentare privind cazuri de utilizare specifice.

---

[5] Raiz Shaffique, M., & van der Hof, S. (2024). *Mapping age assurance typologies and requirements*. *Research report* (Cartografierea tipologiilor și a cerințelor asigurării vârstei. Raport de cercetare), în cadrul proiectului „Un internet mai bun pentru copii” (BIK), coordonat de European Schoolnet (EUN) și comandat de Comisia Europeană.

[6] În ceea ce privește impactul potențial al asigurării vârstei asupra drepturilor și libertăților, a se vedea, de exemplu: “*Roadmap for age verification*” (Foaia de parcurs pentru verificarea vârstei) (Australian eSafety Commissionner, 2023) https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf?v=1731644498261, *„A safe internet by default for children and the role of age verification*” (Un internet sigur implicit pentru copii și rolul verificării vârstei) (AEPD, 2024) https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf sau *„Trustworthy Age Assurance?*” (O asigurare a vârstei de încredere?), un studiu comandat de Grupul Verzilor/ALE privind economia verde și socială la Parlamentul European (2024) https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance.

2. PRINCIPII PRIVIND CONCEPEREA ASIGURĂRII VÂRSTEI ÎN CONFORMITATE CU RGPD

2.1 Exercitarea deplină și efectivă a drepturilor și libertăților

Asigurarea vârstei trebuie să respecte pe deplin drepturile și libertățile fundamentale[7] ale persoanelor fizice, iar interesul superior al copilului ar trebui să prevaleze pentru toate părțile implicate în proces.

10. Atunci când pun în aplicare mecanisme de asigurare a vârstei, furnizorii de servicii ar trebui să se asigure că iau în considerare nu numai impactul asupra dreptului la protecția datelor cu caracter personal, ci și asupra tuturor drepturilor fundamentale ale persoanelor fizice.

11. În cazul specific al copiilor, interesul superior al copilului[8] ar trebui să prevaleze pentru toate părțile implicate în asigurarea vârstei. Este important de reținut faptul că nu există nicio ierarhie în ceea ce privește luarea în considerare a interesului superior al copilului și că ar trebui să se țină seama de toate drepturile copiilor[9], inclusiv de dreptul lor la protecția datelor cu caracter personal, la protecția împotriva violenței și a tuturor celorlalte forme de exploatare, de a avea acces la informații dintr-o varietate de surse și de a se acorda considerația cuvenită opiniilor lor.

2.2 Evaluarea bazată pe riscuri a proporționalității asigurării vârstei

Asigurarea vârstei ar trebui să fie întotdeauna pusă în aplicare într-un mod proporțional și bazat pe riscuri, compatibil cu drepturile și libertățile persoanelor fizice.

12. Furnizorii de servicii ar trebui să adopte o abordare bazată pe riscuri atunci când își concep și furnizează serviciile. Necesitatea și proporționalitatea utilizării măsurilor de siguranță, cum ar fi asigurarea vârstei, ar trebui să se demonstreze ținând seama de riscurile asociate. Necesitatea ar putea fi demonstrată prin efectuarea unei evaluări[10] pentru a identifica și a evalua riscurile pe care un anumit serviciu le prezintă pentru copii[11], cum ar fi expunerea la contacte sau conținuturi nocive. În cadrul acestei evaluări, furnizorii de servicii pot lua în considerare, de asemenea, drepturile copiilor, oportunitățile oferite de mediul digital, opiniile copiilor, precum și capacitățile lor în continuă evoluție, pentru a asigura o participare adecvată vârstei[12].

---

[7] În special, Declarația universală a drepturilor omului, Convenția europeană a drepturilor omului, Carta drepturilor fundamentale a Uniunii Europene și Convenția ONU cu privire la drepturile copilului.

[8] Comitetul ONU pentru drepturile copilului a clarificat faptul că noțiunea de interes superior al copilului *„are ca scop să asigure atât exercitarea deplină și efectivă a tuturor drepturilor recunoscute în Convenție, cât și dezvoltarea holistică a copilului”*. Comentariul general nr. 14 (2013) privind dreptul copilului ca interesul superior al acestuia să prevaleze [articolul 3 alineatul 1], https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.

[9] Comentariul general nr. 25 (2021) privind drepturile copiilor în ceea ce privește mediul digital, OHCHR, martie 2021.

[10] De exemplu, o evaluare a impactului asupra drepturilor copilului („EIDC”), care poate sau nu să facă parte dintr-o EIPD.

[11] Experții în domeniul drepturilor copilului au subliniat beneficiile utilizării evaluărilor impactului asupra drepturilor copilului (EIDC) ca instrument eficace *„pentru transpunerea Convenției [cu privire la drepturile copilului] și a articolului 3 din aceasta, în ceea ce privește tratarea cu prioritate a interesului superior al copilului în practică în mod concret și structurat”* [în Mukherjee, S., Pothong, K., & Livingstone, S. (2021), *Child Rights Impact Assessment: A tool to realise child rights in the digital environment.* (Evaluarea impactului asupra drepturilor copilului: un instrument de punere în aplicare a drepturilor copilului în mediul digital). Londra: 5Rights Foundation]. În plus, Comitetul ONU a invitat statele să mandateze utilizarea EIDC pentru a integra drepturile copiilor în reglementarea și conceperea mediului digital.

[12] Comentariul general nr. 25 (2021) privind drepturile copiilor în ceea ce privește mediul digital, OHCHR, martie 2021.

13. Furnizorii de servicii trebuie, de asemenea, să respecte drepturile și libertățile utilizatorilor lor, inclusiv dreptul la protecția datelor lor cu caracter personal, punându-le în balanță cu nevoia adoptării de măsuri de siguranță, care ar trebui să fie întotdeauna cele mai puțin invazive dintre cele disponibile și care ar trebui să fie întotdeauna eficace. În multe cazuri, asigurarea vârstei prezintă un risc ridicat pentru drepturile și libertățile persoanelor vizate, ceea ce ar necesita, prin urmare, efectuarea unei evaluări a impactului asupra protecției datelor („EIPD", articolul 35 din RGPD) înainte de prelucrare, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării. EIPD ar trebui să includă o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, a interesului legitim urmărit de operator. De asemenea, ar trebui să conțină o evaluare a necesității și proporționalității prelucrării, să identifice riscurile care decurg din prelucrarea datelor cu caracter personal în scopul asigurării vârstei și să conțină măsuri de atenuare a riscurilor respective[13].

14. EIPD ar trebui să ghideze conceperea și punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru respectarea protecției datelor. Această abordare bazată pe riscuri este esențială atunci când se pune în balanță potențiala interferență cu drepturile și libertățile persoanelor fizice și obiectivul urmărit în acest context specific, și anume siguranța copiilor. Domeniul de aplicare, amploarea și intensitatea acestei interferențe în ceea ce privește impactul asupra drepturilor și libertăților trebuie întotdeauna evaluate cu atenție[14]. De exemplu, un furnizor de servicii care prelucrează date cu caracter personal pentru a verifica vârsta tuturor utilizatorilor acestora în momentul accesării tuturor conținuturilor sau serviciilor sale, chiar și atunci când conținuturile sau serviciile sunt adecvate pentru toate categoriile de public și lipsite de orice risc, nu ar trece testele privind necesitatea și proporționalitatea.

2.3 Prevenirea riscurilor în materie de protecție a datelor

Asigurarea vârstei nu ar trebui să conducă la riscuri inutile în materie de protecție a datelor pentru persoanele fizice. În special, asigurarea vârstei nu ar trebui să ofere furnizorilor de servicii mijloace suplimentare de identificare, localizare, creare de profiluri sau urmărire a persoanelor fizice.

15. Furnizorii de servicii și terții implicați în asigurarea vârstei ar trebui să pună în aplicare măsuri și garanții eficace pentru a preveni ca acest proces să genereze riscuri inutile în materie de protecție a datelor, cum ar fi cele care rezultă din identificarea, localizarea, crearea de profiluri sau urmărirea persoanelor fizice. Prelucrarea datelor cu caracter personal pentru asigurarea vârstei nu ar trebui să ofere mijloace suplimentare pentru îndeplinirea unor scopuri care nu au legătură cu asigurarea vârstei în sine. Acest lucru necesită selectarea unor abordări de asigurare a vârstei care să respecte pe deplin principiul protecției datelor începând cu momentul conceperii și în mod implicit (a se vedea secțiunea 2.8) și a unor măsuri de punere în aplicare care să garanteze principiul echității, asigurându-se că datele cu caracter

[13]Orientările CEPD privind evaluarea impactului asupra protecției datelor (EIPD) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679, https://ec.europa.eu/newsroom/article29/items/611236/en.
[14]Orientările AEPD privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

personal nu sunt prelucrate într-un mod în care se aduc prejudicii nejustificate, discriminatoriu din punct de vedere legal, neașteptat sau înșelător pentru persoanele vizate.

16. De exemplu, o persoană fizică care trebuie să se supună unei verificări a vârstei pentru a accesa conținutul pentru adulți nu s-ar aștepta ca furnizorul de servicii să utilizeze asigurarea vârstei pentru a-i stabili identitatea sau localizarea geografică exactă sau pentru a monitoriza, evalua sau deduce aspecte personale ale identității sale. Acest fapt este deosebit de relevant pentru respectarea principiilor de protecție a datelor prevăzute la articolul 5 alineatul (1) din RGPD, inclusiv a principiilor echității, transparenței și limitărilor legate de scop, precum și a normelor prevăzute la articolul 6 alineatul (4) din RGPD privind utilizările ulterioare ale datelor cu caracter personal. În mod similar, în conformitate cu principiile limitărilor legate de scop și reducerii la minimum a datelor prevăzute la articolul 5 alineatul (1) din RGPD, procesul de asigurare a vârstei nu ar trebui să permită vizarea în continuare a utilizatorilor sau crearea de profiluri ale acestora, inclusiv în scopuri comerciale (de exemplu, reclame personalizate), cât și pentru vizarea rău intenționată (de exemplu, ademenirea, bullying-ul, urmărirea în scopul hărțuirii sau hărțuirea). CEPD reamintește că, în temeiul considerentului 75 din RGPD, pot exista riscuri deosebite pentru drepturile în materie de protecție a datelor atunci când datele cu caracter personal se referă la persoane fizice vulnerabile, în special la copii. În general, nu ar trebui să fie posibil să se afle mai mult decât este necesar despre o persoană fizică și acțiunile acesteia prin crearea de profiluri ale persoanei respective pe baza informațiilor utilizate în procesul de asigurare a vârstei. Acest lucru ar trebui asigurat, în cea mai mare măsură posibilă, și în cazul unei încălcări a securității datelor.

17. Situațiile de dezechilibru de putere ar trebui evitate pentru a-i împiedica pe furnizorii de servicii să forțeze persoanele fizice să se confrunte cu riscuri inutile în materie de protecție a datelor din cauza lipsei lor de autoritate[15]. Atunci când nu este posibil, aceste situații trebuie recunoscute și contracarate prin contramăsuri adecvate[16]. De exemplu, utilizatorilor care nu pot sau nu doresc să utilizeze o metodă specifică de asigurare a vârstei ar trebui să li se ofere alternative viabile pentru a face dovada vârstei lor. În plus, furnizorii de servicii ar trebui să evalueze periodic dacă metodele și tehnologiile selectate, inclusiv cele furnizate de terți, funcționează în conformitate cu scopurile lor și să le adapteze pentru a asigura echitatea prelucrării. Terții implicați în asigurarea vârstei ar trebui, de asemenea, să încerce să-i sprijine pe furnizorii de servicii în îndeplinirea obligațiilor care le revin, neintroducând riscuri inutile în materie de protecție a datelor și prin notificarea promptă a oricăror modificări relevante ale politicilor, modelelor, serviciilor etc.

[15] De exemplu, atunci când persoanele vizate se confruntă cu un proces decizional automatizat fără mecanisme de recurs adecvate sau atunci când consimțământul nu poate fi acordat în mod liber. Noțiunea de „dezechilibru de putere” este analizată în cadrul Avizului CEPD nr. 8/2024 privind consimțământul valabil în contextul modelelor de consimțământ sau de plată puse în aplicare de platformele online mari (secțiunea 4.2.1.3), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_ro.pdf.

[16] Din Orientările nr. 3/2022 ale CEPD privind modelele de interfață înșelătoare ale platformelor de comunicare socială: cum să le recunoaștem și să le evităm (secțiunea 2.3), versiunea 2.0, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

2.4 Limitări legate de scop și reducerea la minimum a datelor

Furnizorii de servicii și terții implicați în asigurarea vârstei ar trebui să prelucreze numai atributele legate de vârstă care sunt strict necesare pentru scopul determinat, explicit și legitim al acestora.

18. În majoritatea cazurilor, scopul asigurării vârstei este de a se lua decizii de control al accesului în funcție de vârstă, de a preveni prejudicierea copiilor în mediul online, de a oferi o concepere adecvată sau o experiență adecvată în funcție de vârstă etc. Indiferent de cazul de utilizare, scopul prelucrării datelor cu caracter personal trebuie să fie specific și explicit [articolul 5 alineatul (1) litera (b) din RGPD]. Odată ce datele cu caracter personal sunt colectate, acestea nu pot fi prelucrate ulterior sau combinate cu date suplimentare într-un mod incompatibil cu scopurile respective. Ar trebui utilizate măsuri tehnice, de exemplu tehnologiile de creștere a confidențialității („PET"), pentru a limita posibilitatea de reutilizare a datelor cu caracter personal în alte scopuri. De asemenea, ar trebui puse în aplicare măsuri organizatorice, cum ar fi politici și obligații contractuale, care să limiteze reutilizarea datelor cu caracter personal[17].

19. Un atribut legat de vârstă este orice atribut care indică faptul că o persoană fizică are o anumită vârstă, are peste sau sub o anumită vârstă sau în cadrul unui interval de vârstă. Specificarea scopului va determina atributele relevante și necesare legate de vârstă care trebuie colectate. De asemenea, acest lucru va permite operatorului să evalueze proporționalitatea procesului de asigurare a vârstei. Avantajele care rezultă din acest proces nu ar trebui să fie contrabalansate de niciun dezavantaj în ceea ce privește exercitarea drepturilor fundamentale[18] (a se vedea secțiunea 2.2 de mai sus).

20. Prin urmare, operatorul ar trebui să colecteze numai datele cu caracter personal care sunt necesare, adecvate și relevante pentru scopurile pe care intenționează să le îndeplinească. Astfel, reducerea la minimum a datelor contribuie la justificarea și operaționalizarea principiilor necesității[19] și proporționalității. De exemplu, furnizorul de servicii ar putea avea nevoie să știe doar dacă vârsta utilizatorului este peste sau sub un anumit prag. Această verificare ar putea fi implementată printr-o abordare bazată pe utilizarea unui token cu participarea unui furnizor terț, în care furnizorul de servicii vede doar rezultatul funcțional al procesului de asigurare a vârstei (de exemplu, „peste" sau „sub" pragul de vârstă)[20]. Pot fi relevante alte abordări atunci când furnizorul de servicii trebuie să știe dacă utilizatorul se încadrează într-o anumită categorie de vârstă sau dacă s-a născut într-un anumit an.

[17]Din Orientările CEPD nr. 4/2019 privind articolul 25 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, versiunea 2.0, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[18]Din Orientările AEPD privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[19]Din Evaluarea necesității măsurilor care limitează dreptul fundamental la protecția datelor cu caracter personal: un set de instrumente, AEPD, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

[20]Un furnizor terț efectuează o verificare a vârstei și furnizează utilizatorului un „token legat de vârstă" pe care utilizatorul îl poate prezenta furnizorului de servicii fără a fi necesar să facă dovada vârstei din nou. Tokenul legat de vârstă poate conține diferite atribute ale utilizatorului, precum și informații cu privire la momentul, locul sau modul în care a fost efectuată verificarea vârstei.

2.5 Eficacitatea asigurării vârstei

Asigurarea vârstei ar trebui să atingă, în mod demonstrabil, un nivel de eficacitate adecvat scopului pentru care este efectuată.

21. Mijloacele prin care se realizează asigurarea vârstei ar trebui să fie adecvate pentru atingerea scopului prelucrării. În special, eficacitatea oricărei măsuri de asigurare a vârstei impuse prin lege ar trebui considerată o condiție prealabilă pentru respectarea principiilor necesității[21] și proporționalității[22].

22. Eficacitatea asigurării vârstei ar trebui evaluată cu privire la mai multe aspecte, inclusiv:

a) accesibilitatea. Asigurarea vârstei ar trebui să fie accesibilă pe scară largă persoanelor fizice pentru verificarea vârstei acestora sau pentru a dovedi că acestea îndeplinesc o cerință legată de vârstă. Atunci când anumite categorii de persoane riscă să fie discriminate de o metodă specifică de asigurare a vârstei, de exemplu pentru că nu dețin un document de identitate adecvat sau un telefon mobil sau din cauza unui handicap, ar trebui puse la dispoziție metode alternative de asigurare a vârstei, atunci când acest lucru este rezonabil posibil, cu niveluri adecvate de confidențialitate, siguranță și securitate. Soluțiile de asigurare a vârstei ar trebui, de asemenea, să respecte orice legislație aplicabilă privind accesibilitatea[23];
b) fiabilitatea. În conformitate cu principiul exactității [articolul 5 alineatul (1) litera (d) din RGPD], orice metodă al cărei scop este de a stabili dacă o persoană fizică îndeplinește o cerință legată de vârstă ar trebui să ofere un nivel adecvat și consecvent de exactitate atunci când se stabilește dacă îndeplinește sau nu cerința respectivă. Ar trebui puse la dispoziție mecanisme de recurs adecvate, în special atunci când utilizatorii pot fi afectați în mod semnificativ de procesul decizional automatizat, de exemplu atunci când atributele lor legate de vârstă nu au fost stabilite în mod corespunzător (a se vedea secțiunea 2.7 de mai jos);
c) robustețea. Mecanismul de asigurare a vârstei ar trebui să fie capabil să facă față situațiilor neprevăzute și să reziste încercărilor rezonabile de a păcăli sau de a ocoli sistemul. Trebuie remarcat faptul că robustețea nu are mare relevanță în contextul declarării pe propria răspundere a unui atribut legat de vârstă, deoarece fiabilitatea unei astfel de metode depinde în principal de bunăvoința utilizatorului[24].

În plus, furnizorii de servicii care pun în aplicare asigurarea vârstei și orice terți implicați în proces ar trebui să fie în măsură să demonstreze eficacitatea acesteia și să fie transparenți cu

[21] Evaluarea necesității măsurilor care limitează dreptul fundamental la protecția datelor cu caracter personal: un set de instrumente, AEPD, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

[22] Orientări privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[23] De exemplu, accesibilitatea site-urilor web și a aplicațiilor pentru dispozitive mobile publice și accesibilitatea produselor și serviciilor sunt prevăzute de Directiva privind accesibilitatea site-urilor web (WAD) și, respectiv, de Act european privind accesibilitatea (EAA). Soluțiile de asigurare a vârstei trebuie să asigure conformitatea cu aceste acte legislative, prin îndeplinirea cerințelor standardului european armonizat privind cerințele de accesibilitate pentru produsele și serviciile TIC, EN 301 549 v3.2.1.

[24] CEPD și-a exprimat anterior îndoielile serioase cu privire la eficacitatea declarației pe proprie răspundere ca metodă de verificare a vârstei în contextul prelucrării cu grad ridicat de risc în Decizia obligatorie nr. 2/2023 referitoare la litigiul înaintat de autoritatea de supraveghere irlandeză cu privire la TikTok Technology Limited (articolul 65 din RGPD), https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_ro.

privire la mijloacele prin care ating niveluri adecvate de accesibilitate, fiabilitate și robustețe (a se vedea secțiunea 2.10).

2.6 Legalitate, echitate și transparență

Furnizorii de servicii și terții implicați în asigurarea vârstei ar trebui să se asigure că prelucrarea oricăror date cu caracter personal în scopul asigurării vârstei este legală, echitabilă și transparentă pentru utilizatori.

23. Furnizorii de servicii trebuie să se asigure că au un temei juridic aplicabil în conformitate cu articolul 6 din RGPD [și, dacă este cazul, excepția aplicabilă prevăzută la articolul 9 alineatul (2)] pentru prelucrarea datelor cu caracter personal în contextul asigurării vârstei. De exemplu, aceștia ar putea fi nevoiți să utilizeze asigurarea vârstei în vederea îndeplinirii unei obligații legale [articolul 6 alineatul (1) litera (c) din RGPD], ținând seama de faptul că asigurarea vârstei trebuie să fie proporțională cu obiectivul legitim urmărit și cu cerințele prevăzute la articolul 6 alineatul (3) din RGPD.

24. În plus, furnizorii de servicii trebuie să dea dovadă de transparență în relația cu utilizatorii cu privire la modul exact în care sunt utilizate datele lor cu caracter personal și de către cine. Acest lucru este deosebit de important atunci când există mai multe părți implicate în procesul de asigurare a vârstei. Înainte ca datele cu caracter personal să fie prelucrate în scopul asigurării vârstei, utilizatorii trebuie să fie informați (în temeiul articolelor 12, 13 și 14 din RGPD), printre altele, cu privire la[25]:

- datele cu caracter personal care vor fi prelucrate și modul în care vor fi prelucrate;
- posibilitatea ca în proces să fie implicați terți și, în caz afirmativ, cine sunt aceștia și cine sunt operatorii și persoanele împuternicite de operatori în acest scenariu;
- posibilitatea ca datele lor să fie partajate cu alte persoane sau transferate către o țară terță;
- durata păstrării datelor lor cu caracter personal sau, dacă acest lucru nu este posibil, criteriile de stabilire a perioadei de stocare;
- drepturile lor în legătură cu datele lor cu caracter personal (articolele 15-22 din RGPD), inclusiv modul în care pot contesta o decizie incorectă luată ca urmare a asigurării vârstei.

25. Transparența în contextul asigurării vârstei este deosebit de importantă în ceea ce privește copiii. Furnizorii de servicii trebuie să se asigure că transmit copiilor informații privind transparența, atunci când sunt vizați, într-un mod clar și ușor de înțeles.

26. Conceptul de transparență este legat în mod fundamental de echitate. În cazul în care furnizorii de servicii nu sunt clari și transparenți cu privire la modul în care prelucrează informațiile persoanelor fizice pentru asigurarea vârstei, este puțin probabil ca această prelucrare să poată fi considerată echitabilă, ceea ce, la rândul său, face puțin probabil ca această prelucrare să fie legală. În special, în cazul în care un furnizor oferă utilizatorilor

[25] A se vedea Orientările Grupului de lucru instituit în temeiul articolului 29 privind transparența în temeiul Regulamentului 2016/679, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_ro.pdf.

diferite metode de verificare a vârstei, acesta ar trebui să fie transparent cu privire la impactul pe care îl are fiecare metodă din perspectiva protecției datelor.

2.7 Procesul decizional automatizat

Orice proces decizional automatizat apărut în contextul asigurării vârstei ar trebui să respecte RGPD. Dacă este cazul, furnizorii de servicii și terții implicați ar trebui să prevadă măsuri adecvate pentru protejarea drepturilor, libertăților și a intereselor legitime ale persoanelor fizice.

27. Legiuitorul Uniunii a optat pentru o definiție largă a procesului decizional automatizat, care necesită o examinare de la caz la caz[26]. Deciziile automatizate pot fi implicate în diferite etape ale procesului de asigurare a vârstei, fie pentru accesarea conținutului sau a serviciului, fie prin metodele utilizate pentru a face dovada vârstei.

28. Asigurarea complet automatizată a vârstei poate produce efecte juridice asupra persoanelor fizice în cauză – de exemplu, asupra exercitării libertății lor de exprimare – sau, cel puțin, le poate afecta în mod semnificativ într-un mod similar[27]. Efectul asigurării automatizate a vârstei asupra drepturilor persoanelor fizice poate varia în funcție de tipul de conținut sau de servicii implicate.

29. Prin urmare, furnizorii de servicii și terții implicați în asigurarea vârstei ar trebui să ofere căi de atac și mecanisme de recurs adecvate pentru utilizatorii ale căror atribute legate de vârstă nu sunt stabilite în mod corespunzător. În funcție de arhitectura procesului de asigurare a vârstei, aceștia trebuie să identifice persoanele vizate pe care ar trebui să le contacteze pentru exercitarea drepturilor[28].

30. Furnizorii de servicii și terții implicați ar trebui să acorde o atenție deosebită copiilor. Astfel cum se prevede la considerentul 71 din RGPD, *„luarea de decizii [...] care se bazează exclusiv pe prelucrarea automată [...] care produce efecte juridice în mod similar într-o măsură semnificativă [...] nu ar trebui să se refere la un copil”*. Excepțiile de la această regulă ar trebui să rămână în circumstanțe limitate, cum ar fi atunci când este necesar *„pentru a le proteja bunăstarea”*[29]. În orice caz, furnizorii de servicii și terții implicați ar trebui să pună în aplicare măsuri adecvate – de exemplu, alternative viabile, mecanisme de recurs și, după caz, intervenția umană – cu informații adaptate copiilor, atunci când este cazul.

---

[26]Cauza C-634/21, SCHUFA Holding (Scoring): Hotărârea Curții (Camera întâi) din 7 decembrie 2023 (cerere de decizie preliminară formulată de Verwaltungsgericht Wiesbaden – Germania) – OQ/Land Hessen [Trimitere preliminară – Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal – Regulamentul (UE) 2016/679 – Articolul 22 – Procesul decizional individual automatizat – Societăți care furnizează informații comerciale – Stabilirea automatizată a unei valori de probabilitate în ceea ce privește capacitatea unei persoane de a onora în viitor angajamente de plată („scoring”) – Utilizarea acestei valori de probabilitate de către terți], https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX%3A62021CA0634.

[27]Orientări privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679, https://ec.europa.eu/newsroom/article29/items/612053/en.

[28]Astfel cum se menționează în orientările CEPD (menționate mai sus): *„aceste drepturi oferă suficiente motive pentru o posibilă acționare în judecată a operatorului care creează profilul și a operatorului care ia o decizie automatizată în legătură cu o persoană vizată (cu sau fără intervenție umană), dacă aceste entități nu sunt aceleași”*.

[29]Din Orientările privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679: *„Cu toate acestea, pot să existe circumstanțe în care este necesar ca operatorii să efectueze un proces decizional exclusiv automatizat, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă în legătură cu copiii, de exemplu pentru a le proteja bunăstarea”.*

2.8 Protecția datelor începând cu momentul conceperii și în mod implicit

Asigurarea vârstei ar trebui să fie concepută, pusă în aplicare și evaluată ținând seama de cele mai bune metode și tehnologii disponibile care protejează viața privată pentru a îndeplini cerințele RGPD și a proteja în mod eficace drepturile persoanelor vizate.

31. În temeiul articolului 25 din RGPD, operatorii de date implicați în asigurarea vârstei ar trebui să pună în aplicare măsuri tehnice și organizatorice adecvate și garanțiile necesare pentru a asigura punerea în aplicare în mod eficient a tuturor principiilor de protecție a datelor și, în consecință, a drepturilor și libertăților persoanelor vizate. Cerința ca operatorii să ia în considerare în mod implicit protecția datelor în etapa de proiectare a oricărei activități de prelucrare a datelor cu caracter personal se aplică, de asemenea, persoanelor împuternicite de operatori și pe parcursul întregului ciclu de viață al prelucrării.

32. Având în vedere diversitatea și gravitatea riscurilor asociate sistemelor de asigurare a vârstei, în special atunci când sunt prelucrate documente de identitate sau categorii speciale de date cu caracter personal, cum ar fi datele biometrice, ar trebui acordată cea mai mare atenție pentru a se evita orice acces, prelucrare, partajare și stocare inutilă a datelor cu caracter personal. Sistemele de asigurare a vârstei și orice instrument juridic sau tehnic care stabilește cerințe pentru astfel de sisteme ar trebui, de asemenea, să fie revizuite și actualizate periodic, dacă este necesar, pentru a ține seama de evoluția rapidă a tehnologiilor de îmbunătățire a confidențialității în domeniul gestionării identității digitale.

33. Astfel cum se menționează în orientările CEPD privind protecția datelor începând cu momentul conceperii și în mod implicit[30], trimiterea la „stadiul actual al tehnologiei" în contextul articolului 25 din RGPD impune operatorilor de date obligația de a lua în considerare progresele actuale în ceea ce privește tehnologia care este disponibilă pe piață atunci când stabilesc măsurile tehnice și organizatorice adecvate menționate anterior. Standardele, bunele practici și codurile de conduită care sunt recunoscute de părțile interesate relevante pot fi utile pentru stabilirea unor astfel de măsuri. Cu toate acestea, caracterul adecvat al acestor măsuri ar trebui verificat pentru fiecare activitate de prelucrare în parte.

34. În consecință, CEPD recomandă ca, pe baza stadiului actual al tehnologiei în ceea ce privește asigurarea vârstei la momentul elaborării prezentului document, să se acorde atenția cuvenită tehnologiilor și arhitecturilor care favorizează datele deținute de utilizatori și prelucrarea locală securizată (bazată pe dispozitive), permițând proprietăți precum imposibilitatea de asociere[31] (din punctul de vedere al diferitelor părți și chiar în cazul coluziunilor sau al încălcării securității datelor) și divulgarea selectivă[32] a datelor cu caracter personal sub controlul persoanei vizate. În plus, utilizarea unor abordări precum cele care se

[30] Orientările nr. 4/2019 ale CEPD privind articolul 25 - Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, punctul 2,0, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[31] Proprietatea imposibilității de asociere implică imposibilitatea de a asocia sau corela diferite elemente de date, acțiuni sau tranzacții cu o anumită persoană vizată.

[32] Divulgarea selectivă este o caracteristică a tokenurilor, a acreditărilor și a atestărilor care permite persoanelor vizate să partajeze numai informațiile pe care le doresc cu anumite părți, de la caz la caz.

bazează pe emiterea[33] de loturi de acreditări de unică folosință sau protocoale criptografice, cum ar fi cele de tip zero-knowledge proof[34], ar trebui să fie pusă la dispoziția persoanelor vizate în cazurile în care asigurarea vârstei poate implica riscuri semnificative pentru viața lor privată.

2.9 Securitatea asigurării vârstei

Furnizorii de servicii și terții implicați în asigurarea vârstei ar trebui să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat riscului.

35. RGPD impune atât operatorilor, cât și persoanelor împuternicite de operatori să dispună de măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat riscului la care sunt expuse datele cu caracter personal care sunt prelucrate (considerentul 83 și articolul 32). Natura, sensibilitatea și volumul datelor cu caracter personal care pot fi implicate în asigurarea vârstei evidențiază potențialul efect negativ pe care l-ar putea avea o încălcare a securității datelor.

36. Modelele de încredere sunt esențiale pentru a preveni încălcarea securității datelor în contexte de asigurare a vârstei, deoarece definesc modul în care diferitele părți își pot verifica reciproc identitatea și integritatea. Acestea facilitează comunicarea sigură și schimbul de date între participanți care pot să nu aibă relații anterioare. În plus, pseudonimizarea și criptarea datelor cu caracter personal pot fi măsuri utile pentru atenuarea posibilelor efecte negative ale încălcării securității datelor. Respectarea principiului limitărilor legate de stocare și utilizarea unor perioade scurte de păstrare pot fi, de asemenea, esențiale pentru securitatea asigurării vârstei, reducând suprafața de expunere. O politică privind absența jurnalelor poate fi considerată o garanție valoroasă: odată ce vârsta utilizatorului este verificată, nu se păstrează nicio înregistrare a datelor cu caracter personal utilizate pentru procesul asigurării vârstei.

37. În practică, având în vedere presiunea juridică tot mai mare de a pune în aplicare asigurarea vârstei și numărul de furnizori care pot face obiectul unor astfel de norme, ar trebui să se preconizeze apariția unor încălcări ale securității. Ar trebui să se verifice dacă au fost luate toate măsurile tehnologice de protecție și organizatorice adecvate în scopul de a se stabili imediat dacă s-a produs o încălcare, ceea ce determină în consecință dacă este activată obligația de notificare[35]. Un element-cheie al oricărei politici de securitate a datelor este capacitatea, atunci când este posibil, de a preveni o încălcare și, în cazul în care aceasta se produce, de a reacționa în timp util. Prin urmare, capacitatea de a restabili prompt disponibilitatea asigurării vârstei după o încălcare a securității ar trebui, de asemenea, să fie considerată esențială. În mod similar, este esențial să se asigure reziliența ecosistemului asigurării vârstei, favorizând existența unor alternative diferite și a unor părți între care nu

[33]Emiterea de loturi se bazează pe răspunsul la o cerere de acreditare din partea persoanei vizate cu un set sau un grup de acreditări prezentate în același timp.

[34]Zero-knowledge proof este un protocol în care o parte (autorul) poate demonstra unei alte părți (verificatorul) că o anumită declarație este adevărată, fără a transmite verificatorului nicio informație în afara simplului fapt că afirmația respectivă este adevărată.

[35]Din Orientările CEPD nr. 9/2022 privind notificarea încălcării securității datelor cu caracter personal în temeiul RGPD, https://www.edpb.europa.eu/system/files/2024-11/edpb_guidelines_202209_personal_data_breach_notification_v2.0_ro.pdf.

există relații strânse[36], care nu depind atât de mult unele de altele încât eșecul sau disfuncționalitatea uneia dintre ele să cauzeze limitări semnificative ale accesului.

38. Deși măsurile de securitate sunt extrem de importante pentru asigurarea vârstei, acestea nu garantează că accesul autorizat sau neautorizat la datele cu caracter personal nu va afecta drepturile persoanelor fizice. Acestea nu pot înlocui aplicarea principiilor necesității, proporționalității sau al protecției datelor începând cu momentul conceperii și în mod implicit.

2.10 Responsabilitate

Furnizorii de servicii și terții implicați ar trebui să pună în aplicare metode de guvernanță care să le permită să fie răspunzători pentru abordarea lor în ceea ce privește asigurarea vârstei și pentru demonstrarea conformității lor cu reglementările privind protecția datelor și cu alte cerințe legale.

39. Având în vedere implicarea diferitelor părți interesate, guvernanța asigurării vârstei joacă un rol esențial în asumarea responsabilității. Asigurarea vârstei ar trebui să funcționeze în temeiul unui cadru de guvernanță care să asigure faptul că toate procesele și sistemele sunt concepute, puse în aplicare, revizuite, documentate, evaluate, utilizate, întreținute, testate sau auditate într-un mod care respectă reglementările privind protecția datelor și alte cerințe legale. Acest cadru ar trebui să includă cel puțin politicile de protecție a datelor [articolul 24 alineatul (2) din RGPD] și procesele de stabilire a priorităților și de luare a deciziilor necesare pentru atingerea obiectivelor de conformitate și pentru gestionarea adecvată a riscurilor pe parcursul întregului ciclu de viață al asigurării vârstei.

40. De exemplu, cadrul de guvernanță ar trebui să definească cine și în ce mod este responsabil, din perspectiva operatorului/persoanei împuternicite de operator, pentru ce activități sau operațiuni exacte din cadrul prelucrării. De asemenea, ar trebui să se asigure că asigurarea vârstei poate fi auditată în mod eficace de către autorități și părțile interesate relevante. Cadrul de guvernanță este esențial pentru responsabilitate, dar și pentru transparență și încredere în asigurarea vârstei. Probabilitatea este mai mare ca persoanele vizate să aibă încredere în metode care sunt transparente în ceea ce privește operațiunile lor, procesul decizional etc.

41. În plus, o parte a cadrului de guvernanță implică asigurarea eficacității (secțiunea 2.5), a protecției adatelor începând cu momentul conceperii și în mod implicit (secțiunea 2.8) și a securității (secțiunea 2.9) asigurării vârstei.

[36]Părțile depind una de alta în cea mai mică măsură posibilă, reducând domeniul de aplicare al impactului atunci când apar modificări sau disfuncționalități.

Pentru Comitetul European pentru Protecția Datelor,

Președinte

(Anu Talus)