

Statement



Translations proofread by EDPB Members.
This language version has not yet been proofread.

Paziņojums Nr. 1/2025 par vecuma apstiprināšanu

Pieņemts 2025. gada 11. februārī¹

Eiropas Datu aizsardzības kolēģija ir pieņēmusi šādu paziņojumu:

1. PAZIŅOJUMA KONTEKSTS UN MĒRĶIS

1. Eiropas tiesiskais regulējums aicina pastiprināt bērnu aizsardzību digitālajā vidē. Piemēram, Audiovizuālo mediju pakalpojumu direktīvā², ko dalībvalstis ir transponējušas savos tiesību aktos, ir uzsvērtā iespēja īstenot vecuma pārbaudes pasākumus (6.a un 28.b pants), VDAR ievieš minimālā vecuma prasības, lai piekristu personas datu apstrādei saistībā ar informācijas sabiedrības pakalpojumiem (8. pants), Digitālo pakalpojumu aktā³ kā riska mazināšanas pasākums ir minēta vecuma pārbaude (35. panta 1. punkts), un vairākas dalībvalstis savos tiesību aktos ir ieviesušas minimālā vecuma prasības juridisku darbību veikšanai, konkrētu tiesību īstenošanai vai piekļuvei konkrētām precēm un pakalpojumiem.
2. Turklāt dažādās valstu un Eiropas iniciatīvās, piemēram, “Bērniem labāks internets” (BIK+), vecuma apstiprināšana ir identificēta kā viens no risinājumiem, kā uzlabot bērnu labbūtību tiešsaistē, izmantojot drošu, vecumam piemērotu digitālo vidi saskaņā ar Eiropas digitālajām tiesībām un principiem⁴.

¹ 2025. gada 24. februārī šā dokumenta formatējumā tika veikti nelieli labojumi. 2025. gada 1. aprīlī 16. punktā un 22. punkta b) apakšpunktā papildus tika veiktas nelielas izmaiņas.

² Eiropas Parlamenta un Padomes Direktīva (ES) 2018/1808 (2018. gada 14. novembris), ar ko, ņemot vērā mainīgos tirgus apstākļus, groza Direktīvu 2010/13/ES par to, lai koordinētu dažus dalībvalstu normatīvajos un administratīvajos aktos paredzētus noteikumus par audiovizuālo mediju pakalpojumu sniegšanu (Audiovizuālo mediju pakalpojumu direktīva), <https://eur-lex.europa.eu/eli/dir/2018/1808/oj>.

³ Eiropas Parlamenta un Padomes Regula (ES) 2022/2065 (2022. gada 19. oktobris) par digitālo pakalpojumu vienoto tirgu un ar ko groza Direktīvu 2000/31/EK (Digitālo pakalpojumu akts) <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.

⁴ Labāks internets bērniem, Rokasgrāmata par vecuma apstiprināšanu, <https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest>.

3. Pamatojoties uz definīciju, kas sniegta izpētes ziņojumā *Mapping age assurance typologies and requirements*⁵ (Vecuma apstiprināšanas tipoloģiju un prasību kartēšana), šajā dokumentā jēdziens “vecuma apstiprināšana” tiks lietots kā “vispārējs termins, kas attiecas uz metodēm, ko izmanto, lai noteiktu indivīda vecumu vai vecuma diapazonu līdz dažādiem ticamības vai noteiktības līmeņiem”. Tajā pašā ziņojumā ir minētas trīs galvenās vecuma apstiprināšanas kategorijas: vecuma noteikšana, vecuma pārbaude un pašdeklarācija.
4. Vecuma apstiprināšanas prasība rada īpašus riskus datu aizsardzībai, jo var negatīvi ietekmēt ne tikai fizisko personu tiesības uz savu personas datu aizsardzību, bet arī citas tiesības un brīvības⁶, piemēram, tiesības uz nediskrimināciju, tiesības uz personas neaizskaramību, tiesības uz brīvību un drošību un tiesības uz vārda un informācijas brīvību.
5. Atzīstot, cik svarīga ir konsekventa pieeja ES līmenī vecuma apstiprināšanas jautājumam, EDAK vēlas sniegt konkrētus norādījumus un nodrošināt augsta līmeņa principus, kas izriet no VDAR un kas būtu jāņem vērā, apstrādājot personas datus vecuma apstiprināšanas kontekstā.
6. Ierosināto principu mērķis ir saskaņot bērnu aizsardzību ar personas datu aizsardzību vecuma apstiprināšanas kontekstā.
7. Prioritāte ir piešķirta prasībām attiecībā uz VDAR 5. pantā noteiktajiem galvenajiem principiem (likumīgums, godprātība, pārredzamība, nolūka ierobežojums, datu minimizēšana, precizitāte, glabāšanas ierobežojums, konfidencialitāte, integritāte un pārskatatbildība), un tam, lai nodrošinātu, ka šie datu aizsardzības principi tiek pienācīgi īstenoti un laika gaitā paliek stingri, kā noteikts VDAR 25. pantā “Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma” un VDAR 32. pantā “Apstrādes drošība”.
8. Šajā paziņojumā ir aplūkoti principi, kas piemērojami dažādiem tiešsaistes lietošanas gadījumiem, arī gadījumos, kad minimālais vecums ir noteikts tiesību aktos vai citādi kā kritērijs, lai varētu iegādāties produktus, izmantot pakalpojumus, kas varētu kaitēt bērniem, vai veikt juridiskas darbības, un ja ir pienākums rūpēties par bērnu aizsardzību (piemēram, nodrošināt, ka pakalpojumi tiek izveidoti vai piedāvāti vecumam atbilstošā veidā).
9. EDAK var arī apsvērt iespēju – attiecīgā gadījumā un citos dokumentos – sniegt papildu norādījumus par konkrētiem lietošanas gadījumiem.

⁵ Raiz Shaffique, M., un van der Hof, S. (2024). *Mapping age assurance typologies and requirements*. Izpētes ziņojums ir daļa no projekta “Bērniem labāks internets” (BIK), ko koordinē European Schoolnet (EUN) un ko ir pasūtījusi Eiropas Komisija.

⁶ Par vecuma apstiprināšanas prasības iespējamo ietekmi uz tiesībām un brīvībām sk., piemēram: “Roadmap for age verification” (Austrālijas e-drošības komisārs, 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” (AEPD, 2024) <https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf> vai “Trustworthy Age Assurance?” pētījums par zaļo un sociālo ekonomiku, ko pasūtījusi Eiropas Parlamenta Zaļo un Eiropas Brīvās apvienības grupa (2024) <https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance>.

2. VDAR PRASĪBĀM ATBILSTOŠAS VECUMA APSTIPRINĀŠANAS IZVEIDES PRINCIPI

2.1 Tiesību un brīvību pilnīga un efektīva izmantošana

Vecuma apstiprināšanas procesā ir pilnībā jāņem vērā fizisko personu pamattiesības⁷ un brīvības, un bērnu interesēm vajadzētu būt primārajam apsvērumam visām vecuma apstiprināšanas procesā iesaistītajām personām.

10. Īstenojot vecuma apstiprināšanas procesu, pakalpojumu sniedzējiem būtu jānodrošina, ka tie ņem vērā ne tikai ietekmi uz tiesībām uz personas datu aizsardzību, bet arī ietekmi uz visām fizisko personu pamattiesībām.
11. Bērnu gadījumā bērna interesēm⁸ vajadzētu būt primārajam apsvērumam visām vecuma apstiprināšanas nodrošināšanā iesaistītajām personām. Ir svarīgi atzīmēt, ka nav bērna interešu ievērošanas hierarhijas, un būtu jāņem vērā visas bērnu tiesības⁹, arī tiesības uz personas datu aizsardzību, aizsardzību pret vardarbību un visiem citiem izmantošanas veidiem, tiesības piekļūt informācijai no dažādiem avotiem un tas, lai bērnu viedoklis tiktu pienācīgi ņemts vērā.

2.2 Uz risku balstītas vecuma apstiprināšanas samērīguma novērtējums

Vecuma apstiprināšana vienmēr būtu jāīsteno uz risku balstītā un samērīgā veidā, kas ir saderīgs ar fizisko personu tiesībām un brīvībām.

12. Pakalpojumu sniedzējiem, plānojot un sniedzot savus pakalpojumus, būtu jāpieņem uz risku balstīta pieeja. Būtu jāpierāda drošības pasākumu, piemēram, vecuma apstiprināšanas, izmantošanas nepieciešamība un samērīgums, ņemot vērā ar to saistītos riskus. Nepieciešamību varētu pierādīt, veicot novērtējumu¹⁰, lai noteiktu un novērtētu riskus, ko konkrēts pakalpojums rada bērniem¹¹, piemēram, pakļaušanu kaitīgai saskarei vai saturam. Minētā novērtējuma ietvaros pakalpojumu sniedzēji var ņemt vērā arī bērnu tiesības, digitālās vides sniegtās iespējas, bērnu viedokļus, kā arī viņu spēju attīstību, lai nodrošinātu vecumam atbilstošu līdzdalību¹².
13. Pakalpojumu sniedzējiem ir arī jāievēro lietotāju tiesības un brīvības, arī tiesības uz personas datu aizsardzību, un tās jālīdzsvaro ar tādiem drošības pasākumiem no pieejamo vidus, kuri rada vismazāko iejaukšanos un kuriem vienmēr vajadzētu būt efektīviem. Daudzos gadījumos

⁷ Īpaši Vispārējā cilvēktiesību deklarācija, Eiropas Cilvēktiesību konvencija, Eiropas Savienības Pamattiesību harta un ANO Konvencija par bērna tiesībām.

⁸ ANO Bērna tiesību komiteja ir precizējusi, ka interešu principa "mērķis ir nodrošināt visu konvencijā atzīto tiesību pilnīgu un efektīvu izmantošanu un bērna holistisku attīstību". Vispārējais komentārs Nr. 14 (2013) par bērnu tiesībām uz to, lai primārais apsvērumu būtu viņu intereses (3. panta 1. punkts), https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.

⁹ Vispārējais komentārs Nr. 25 (2021) par bērnu tiesībām saistībā ar digitālo vidi, OHCHR, 2021. gada marts.

¹⁰ Piemēram, novērtējums par ietekmi uz bērna tiesībām ("CRIA"), kas var būt vai nebūt NIDA daļa.

¹¹ Eksperti bērnu tiesību jomā ir uzsvēruši ieguvumus, ko sniedz novērtējuma par ietekmi uz bērna tiesībām (CRIA) kā lietderīga instrumenta izmantošana, "lai Konvenciju [par bērnu tiesībām] un tās 3. pantu par prioritātes piešķiršanu bērna interesēm pārvērstu praksē konkrētā un strukturētā veidā" (Mukherjee, S., Pothong, K., & Livingstone, S. (2021)). *Child Rights Impact Assessment: A tool to realise child rights in the digital environment*, Londona, 5Rights Foundation). Turklāt ANO komiteja ir aicinājusi valstis atļaut izmantot CRIA, lai iekļautu bērnu tiesības digitālās vides regulējumā un izstrādē.

¹² Vispārējais komentārs Nr. 25 (2021) par bērnu tiesībām saistībā ar digitālo vidi, OHCHR, 2021. gada marts.

vecuma apstiprināšanas prasība rada augstu risku datu subjektu tiesībām un brīvībām, tāpēc pirms apstrādes būtu jāveic novērtējums par ietekmi uz datu aizsardzību ("NIDA", VDA 35. pants), ņemot vērā apstrādes raksturu, tvērumu, kontekstu un nolūkus. NIDA būtu sistemātiski jāapraksta paredzētās apstrādes darbības un apstrādes nolūki, ieskaitot – attiecīgā gadījumā – pārziņa leģitīmās intereses. Aprakstā būtu jāietver arī apstrādes nepieciešamības un samērīguma novērtējums, jāapzina riski, kas izriet no personas datu apstrādes vecuma apstiprināšanas nolūkā, un jāietver pasākumi minēto risku mazināšanai¹³.

14. NIDA būtu jāsniedz norādījumi par atbilstošu tehnisko un organizatorisko pasākumu izstrādi un īstenošanu, lai nodrošinātu atbilstību datu aizsardzības prasībām. Šī uz risku balstītā pieeja ir būtiska, lai iespējamo iekļaušanos fizisko personu tiesībās un brīvībās šajā konkrētajā kontekstā līdzsvarotu ar paredzēto mērķi, proti, bērnu drošību. Vienmēr ir rūpīgi jāizvērtē šīs iekļaušanās tvērums, apjoms un intensitāte attiecībā uz ietekmi uz tiesībām un brīvībām¹⁴. Piemēram, ja pakalpojumu sniedzējs, kurš apstrādā personas datus, lai pārbaudītu visu pakalpojumu lietotāju vecumu, kad tie piekļūst visam saturam vai pakalpojumiem, pat ja saturs vai pakalpojumi ir piemēroti visām auditorijām un nerada nekādu risku, neveiktu nepieciešamības un samērīguma pārbaudes.

2.3 Datu aizsardzības risku novēršana

Vecuma apstiprināšanai nevajadzētu radīt nevajadzīgus datu aizsardzības riskus fiziskām personām. Vecuma apstiprināšanai jo īpaši nebūtu jārada papildu līdzekļi pakalpojumu sniedzējiem fizisko personu identificēšanai, atrašanās vietas noteikšanai, profilēšanai vai izsekošanai.

15. Pakalpojumu sniedzējiem un visām trešām personām, kas iesaistītas vecuma apstiprināšanas procesā, būtu jāīsteno efektīvi pasākumi, lai samazinātu aizsardzības riskus, piemēram, tādus, kas izriet no fizisku personu identificēšanas, atrašanās vietas noteikšanas, profilēšanas vai izsekošanas. Personas datu apstrādei vecuma apstiprināšanas nolūkā nebūtu jārada papildu līdzekļi, lai īstenotu nolūkus, kas nav saistīti ar pašu vecuma apstiprināšanu. Lai to panāktu, ir jāizvēlas tādas vecuma apstiprināšanas pieejas, kas pilnībā atbilst integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principam (sk. 2.8. iedaļu), un jāīsteno pasākumi, kuri garantē godprātības principa ievērošanu un tādējādi nodrošina, ka personas dati netiek apstrādāti tādā veidā, kas datu subjektiem rada nepamatotu kaitējumu, ir prettiesiski diskriminējošs, negaidīts vai maldinošs.
16. Piemēram, fiziska persona, kurai jāapstiprina savs vecums, lai piekļūtu pieaugušajiem paredzētam saturam, negaidītu, ka pakalpojumu sniedzējs izmantos vecuma apstiprināšanu nolūkā noteikt personas identitāti vai precīzu ģeogrāfisko atrašanās vietu vai novērot,

¹³ EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (EDAK pamatnostādnes par novērtējumu par ietekmi uz datu aizsardzību (NIDA) un kas nosaka, vai apstrāde "var radīt augstu risku" Regulas 2016/679 piemērošanas nolūkā), <https://ec.europa.eu/newsroom/article29/items/611236/en>.

¹⁴ EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (EDAU pamatnostādnes par to pasākumu samērīguma novērtēšanu, kuri ierobežo pamattiesības uz privātumu un personas datu aizsardzību), https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

novērtēt vai izsecināt personiskus identitātes aspektus. Šis fakts ir īpaši svarīgs, lai nodrošinātu atbilstību datu aizsardzības principiem saskaņā ar VDAR 5. panta 1. punktu, tai skaitā godprātības, pārredzamības un nolūka ierobežojuma principam, un VDAR 6. panta 4. punkta noteikumiem par personas datu turpmāku izmantošanu. Tāpat, ievērojot nolūka ierobežojuma un datu minimizēšanas principus saskaņā ar VDAR 5. panta 1. punktu, vecuma apstiprināšanas procesam nevajadzētu dot iespēju veikt lietotāju turpmāku mērķorientēšanu vai profilēšanu, arī komerciālu (piemēram, vērstu uz personalizētām reklāmām) un ļaunprātīgu mērķorientēšanu (piemēram, vērstu uz iedraudzināšanu, iebiedēšanu, vajāšanu vai aizskaršanu). EDAK atgādina, ka saskaņā ar VDAR 75. apsvērumu var pastāvēt īpaši riski datu aizsardzības tiesībām, ja personas dati attiecas uz neaizsargātām fiziskām personām, īpaši bērniem. Kopumā nevajadzētu būt iespējai uzzināt vairāk nekā vajadzīgs par fizisko personu un tās darbībām, profilējot šo personu, pamatojoties uz vecuma apstiprināšanas procesā izmantoto informāciju. Tas, cik vien iespējams, būtu jānodrošina arī datu aizsardzības pārkāpuma gadījumā.

17. Būtu jāizvairās no spēku nelīdzsvarotības situācijām, lai novērstu to, ka pakalpojumu sniedzēji piespiež personas saskarties ar nevajadzīgiem datu aizsardzības riskiem, jo tām trūkst pārstāvības¹⁵. Ja tas nav iespējams, šīs situācijas būtu jāatpazīst un uz tām būtu jāreaģē ar piemērotiem pretpasākumiem¹⁶. Piemēram, būtu jānodrošina dzīvotspējīgas alternatīvas vecuma pierādīšanai tiem lietotājiem, kuri nevar vai nevēlas izmantot konkrētu vecuma apstiprināšanas metodi. Turklāt pakalpojumu sniedzējiem būtu regulāri jānovērtē, vai izvēlētās metodes un tehnoloģijas, ieskaitot tās, kuras nodrošina trešās personas, darbojas atbilstoši to nolūkiem, un jāpielāgo tās, lai nodrošinātu godprātību apstrādē. Vecuma apstiprināšanas procesā iesaistītajām trešām personām būtu arī jācenšas palīdzēt pakalpojumu sniedzējiem pildīt savus pienākumus tādā veidā, lai netiktu radīti nevajadzīgi datu aizsardzības riski un savlaicīgi tiktu paziņots par jebkādam attiecīgām izmaiņām to politikā, struktūrā, pakalpojumos u. c.

2.4 Nolūka ierobežojumi un datu minimizēšana

Pakalpojumu sniedzējiem un jebkurai trešai personai, kura iesaistīta vecuma apstiprināšanas procesā, būtu jāapstrādā tikai tie ar vecumu saistītie atribūti, kas ir absolūti nepieciešami to konkrētajam, skaidrajam un leģitīmajam nolūkam.

18. Vairumā gadījumu vecuma apstiprināšanas nolūks ir pieņemt ar vecumu saistītus piekļuves kontroles lēmumus, novērst kaitējumu bērniem tiešsaistē, piedāvāt atbilstošu dizainu vai pieredzi atbilstoši vecumam utt. Neatkarīgi no izmantošanas gadījuma personas datu apstrādes nolūkam vajadzētu būt konkrētam un skaidram (VDAR 5. panta 1. punkta b) apakšpunkts). Kad personas dati ir savākti, tos tālāk neapstrādā vai nekombinē ar papildu datiem tādā veidā, kas nav savienojams ar minētajiem nolūkiem. Lai ierobežotu personas datu pārprofilēšanas iespēju, būtu jāizmanto tādi tehniski pasākumi kā privātuma uzlabošanas

¹⁵ Piemēram, ja datu subjekti saskaras ar automatizētu lēmumu pieņemšanu bez pienācīgiem tiesiskās aizsardzības mehānismiem vai ja tie nevar brīvi sniegt piekrišanu. "Spēku nevienlīdzības" jēdziens ir aplūkots EDAK Atzinumā 08/2024 par derīgu piekrišanu lielo tiešsaistes platformu īstenoto modeļu "piekrist vai maksāt" kontekstā (4.2.1.3. iedaļa), https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

¹⁶ EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (EDAK Pamatnostādnes 03/2022 par maldinošām saskarnēm sociālo mediju platformu saskarnēs – kā tās atpazīt un novērst) (2.3. iedaļa), versija 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.

tehnoloģijas ("PET"). Būtu jāievieš arī organizatoriski pasākumi, piemēram, politika un līgumsaistības, kas ierobežo personas datu atkalizmantošanu¹⁷.

19. Ar vecumu saistīta īpašība ir jebkurš atribūts, kas norāda, ka fiziska persona ir konkrētā vecumā, ir pārsniegusi vai nav sasniegusi noteiktu vecumu vai ietilpst vecuma grupā. Nolūka specifikācijā tiks noteikti attiecīgie un nepieciešamie ar vecumu saistītie atribūti, kas ir jāvērtē. Tas arī ļaus pārzinim novērtēt vecuma apstiprināšanas procesa samērīgumu. Priekšrocībām, kas izriet no šī procesa, nevajadzētu būt mazākām nekā trūkumiem attiecībā uz pamattiesību īstenošanu¹⁸ (sk. 2.2. iedaļu iepriekš).
20. Tāpēc pārzinim būtu jāvērtē tikai tādi personas dati, kas ir nepieciešami, adekvāti un atbilstīgi paredzētajiem nolūkiem. Tādējādi datu minimizēšana palīdz pamatot un īstenot nepieciešamības¹⁹ un samērīguma principus. Piemēram, pakalpojumu sniedzējam varētu būt tikai jāzina, vai lietotājs ir pārsniedzis vai nav sasniegjis noteiktu vecuma sliekšni. To varētu īstenot, izmantojot marķierierīces pieeju, kuras pamatā ir trešās personas – pakalpojumu sniedzēja līdzdalība un kurā pakalpojumu sniedzējs redz tikai vecuma apstiprināšanas procesa funkcionālo rezultātu (piemēram, "pārsniedz" vai "nav sasniegjis" vecuma sliekšni)²⁰. Dažādas pieejas var būt svarīgas, ja pakalpojumu sniedzējam ir jāzina, vai lietotājs ir konkrētā vecuma grupā vai dzimis konkrētā gadā.

2.5 Vecuma apstiprināšanas efektivitāte

Vecuma apstiprināšanai būtu uzskatāmi jāsasniedz tāds efektivitātes līmenis, kas atbilst nolūkam, kuram tā tiek veikta.

21. Līdzekļiem, ar kuriem veic vecuma apstiprināšanu, vajadzētu būt pietiekamiem, lai sasniegtu apstrādes nolūku. Jo īpaši, jebkura juridiski atļauta vecuma apstiprināšanas pasākuma efektivitāte būtu jāuzskata par priekšnosacījumu nepieciešamības²¹ un proporcionalitātes²² principu ievērošanai.

¹⁷EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (EDAK Pamatnostādnes 4/2019 par 25. pantu par integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma), versija 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.

¹⁸EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (EDAU pamatnostādnes par to pasākumu samērīguma novērtēšanu, kuri ierobežo pamattiesības uz privātumu un personas datu aizsardzību), https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

¹⁹EDPS toolkit for Assessing the necessity of measures that limit the fundamental right to the protection of personal data (EDAU rīkkopa tādu pasākumu nepieciešamības novērtēšanai, kas ierobežo pamattiesības uz personas datu aizsardzību), https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²⁰Trešā persona – pakalpojumu sniedzējs veic vecuma pārbaudi un nodrošina lietotājam "vecuma marķierierīci", ko lietotājs var uzrādīt pakalpojumu sniedzējam bez nepieciešamības vēlreiz pierādīt savu vecumu. Vecuma marķierierīcē var būt dažādi lietotāja atribūti un informācija par to, kad, kur un kā veikta vecuma pārbaude.

²¹EDPS toolkit for Assessing the necessity of measures that limit the fundamental right to the protection of personal data (EDAU rīkkopa tādu pasākumu nepieciešamības novērtēšanai, kas ierobežo pamattiesības uz personas datu aizsardzību), https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²²Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Pamatnostādnes par to pasākumu samērīguma novērtēšanu, kuri ierobežo pamattiesības uz privātumu un personas datu aizsardzību), https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

22. Vecuma apstiprināšanas efektivitāte būtu jānovērtē, ņemot vērā vairākus turpmāk norādītos aspektus.

- a) Pieklūstamība. Vecuma apstiprināšanas metodei vajadzētu būt plaši pieejamai fiziskām personām, lai apstiprinātu savu vecumu vai pierādītu, ka tās atbilst ar vecumu saistītām prasībām. Ja, izmantojot kādu vecuma apstiprināšanas metodi, konkrētas personu kategorijas ir pakļautas riskam tikt diskriminētām, piemēram, tāpēc, ka tām nav piemērota personu apliecinoša dokumenta vai nepieder moblais tālrunis, vai invaliditātes dēļ, būtu jādara pieejamas alternatīvas vecuma apstiprināšanas metodes (ja tas ir praktiski iespējams) ar atbilstošu privātuma, drošuma un drošības līmeni. Vecuma apstiprināšanas risinājumiem vajadzētu būt atbilstošiem arī visiem piemērojamiem tiesību aktiem par pieklūstamību²³.
- b) Uzticamība. Saskaņā ar precizitātes principu (VDAR 5. panta 1. punkta d) punkts) jebkurai metodei, kuras mērķis ir noteikt, vai fiziska persona atbilst ar vecumu saistītām prasībām, būtu jānodrošina atbilstošs un konsekvents precizitātes līmenis, kad tiek noteikts, vai persona atbilst minētajai prasībai. Būtu jādara pieejami atbilstoši tiesiskās aizsardzības mehānismi, īpaši tad, ja automatizēta lēmumu pieņemšana var būtiski ietekmēt lietotājus, piemēram, ja viņu ar vecumu saistītie atribūti nav pienācīgi noteikti (sk. 2.7. iedaļu).
- c) Noturība. Vecuma apstiprināšanas procesā vajadzētu spēt risināt neparedzētas situācijas un pretoties iespējamiem mēģinājumiem sagraut vai apiet sistēmu. Jānorāda, ka noturībai ir maza nozīme saistībā ar pašdeklarāciju par atribūtu, kas saistīts ar vecumu, jo šādas metodes uzticamība galvenokārt ir atkarīga no lietotāja labās gribas²⁴.

Turklāt pakalpojumu sniedzējiem, kuri īsteno vecuma apstiprināšanu, un visām procesā iesaistītajām trešām personām būtu jāspēj pierādīt šīs metodes efektivitāti un jābūt pārredzamām attiecībā uz līdzekļiem, ar kuriem tiek sasniegts atbilstīgs pieklūstamības, uzticamības un noturības līmenis (sk. 2.10. iedaļu).

2.6 Likumība, godprātība un pārredzamība

Pakalpojumu sniedzējiem un visām trešām personām, kas iesaistītas vecuma apstiprināšanas procesā, būtu jānodrošina, ka personas datu apstrāde vecuma apstiprināšanas nolūkā tiek veikta likumīgā, godprātīgā un lietotājiem pārredzamā veidā.

23. Pakalpojumu sniedzējiem ir jānodrošina, ka tiem ir piemērojams juridiskais pamats saskaņā ar VDAR 6. pantu (un attiecīgā gadījumā 9. panta 2. punktā paredzētais piemērojamais izņēmums) personas datu apstrādei vecuma apstiprināšanas kontekstā. Piemēram, tām var būt nepieciešams ieviest vecuma apstiprināšanu, lai izpildītu juridisku pienākumu (VDAR 6. panta 1. punkta c) apakšpunkts), ņemot vērā, ka vecuma apstiprināšanai ir jābūt samērīgai ar izvirzīto leģitīmo mērķi un VDAR 6. panta 3. punktā noteiktajām prasībām.

²³ Piemēram, publiskā sektora tīmekļa vietņu un mobilo lietotņu pieklūstamība un produktu un pakalpojumu pieklūstamība ir paredzēta attiecīgi Tīmekļa pieklūstamības direktīvā (WAD) un Eiropas Pieklūstamības aktā (EAA). Ir jānodrošina vecuma apstiprināšanas risinājumu atbilstība minētajiem tiesību aktiem, kas tiek panākts, izpildot prasības, kas minētas saskaņotajā Eiropas standartā (EN 301 549 v3.2.1.) par IKT produktu un pakalpojumu pieklūstamības prasībām.

²⁴ EDAK iepriekš ir paudusi nopietnas šaubas par pašdeklarācijas kā vecuma pārbaudes metodes efektivitāti augsta riska apstrādes kontekstā saistošajā lēmumā 2/2023 par strīdu, ko Īrijas UI iesniegusi attiecībā uz *TikTok Technology Limited* (VDAR 65. pants), https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf.

24. Turklāt pakalpojumu sniedzējiem ir jānodrošina pārredzamība lietotājiem attiecībā uz to, kā un kas tieši izmanto viņu personas datus. Tas ir īpaši svarīgi, ja vecuma apstiprināšanas procesā ir iesaistītas vairākas personas. Pirms jebkādu personas datu apstrādes vecuma apstiprināšanas nolūkā lietotāji ir jāinformē (saskaņā ar VDAR 12., 13. un 14. pantu) cita starpā par to²⁵:
- kādi personas dati tiks apstrādāti un kā tos apstrādās;
 - vai procesā tiks iesaistītas trešās personas un, ja tās ir iesaistītas, tad kas tās ir un kas ir pārziņi un apstrādātāji šajā scenārijā;
 - vai viņu dati tiks kopīgoti ar citiem vai nosūtīti trešai valstij;
 - cik ilgi tiks glabāti viņu personas dati, vai, ja tas nav iespējams, par kritērijiem glabāšanas perioda noteikšanai;
 - kādas ir viņu tiesības attiecībā uz viņu personas datiem (VDAR 15.–22. pants), arī to, kā viņi var apstrīdēt nepareizu lēmumu, kas pieņemts vecuma apstiprināšanas rezultātā.
25. Pārredzamība vecuma apstiprināšanas kontekstā ir īpaši svarīga attiecībā uz bērniem. Pakalpojumu sniedzējiem jānodrošina, ka pārredzamības informācija bērniem tiek sniegta skaidrā un viegli saprotamā veidā.
26. Pārredzamības jēdziens ir fundamentāli saistīts ar godprātību. Ja pakalpojumu sniedzēji nesniedz skaidru un pārredzamu informāciju par to, kā tie vecuma apstiprināšanas nolūkā apstrādā fizisko personu informāciju, tad ir maz ticams, ka šo apstrādi var uzskatīt par godprātīgu, kas savukārt padara maz ticamu, ka šī apstrāde ir likumīga. Īpaši tad, ja pakalpojumu sniedzējs piedāvā lietotājiem dažādas metodes vecuma apstiprināšanai, tam vajadzētu nodrošināt pārredzamību attiecībā uz katras metodes ietekmi no datu aizsardzības viedokļa.

2.7 Automatizēta lēmumu pieņemšana

Visiem gadījumiem, kad vecuma apstiprināšanas kontekstā tiek pieņemti automatizēti lēmumi, vajadzētu būt atbilstošiem VDAR. Attiecīgā gadījumā pakalpojumu sniedzējiem un visām iesaistītajām trešām personām būtu jānodrošina piemēroti pasākumi, lai aizsargātu fizisko personu tiesības un brīvības un leģitīmās intereses.

27. ES likumdevējs ir izvēlējis plašu automatizētas lēmumu pieņemšanas definīciju, kas ir jāizskata katrā gadījumā atsevišķi²⁶. Automatizētus lēmumus var izmantot dažādos vecuma apstiprināšanas procesa posmos – vai nu piekļuvei saturam vai pakalpojumam, vai, kad tiek izmantotas metodes vecuma pierādīšanai.
28. Pilnībā automatizēta vecuma apstiprināšana var radīt tiesiskas sekas attiecīgajām fiziskajām personām, piemēram, vārda brīvības īstenošanai, vai vismaz var būtiski ietekmēt tās līdzīgā

²⁵ Sk. 29. panta darba grupas pamatnostādnes par pārredzamību saskaņā ar Regulu 2016/679, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf.

²⁶ Lieta C-634/21 *SCHUFA Holding* (Kredītpējas vērtējums (*Scoring*)): Tiesas (pirmā palāta) 2023. gada 7. decembra spriedums (*Verwaltungsgericht Wiesbaden* (Vācija) lūgums sniegt prejudiciālu nolēmumu) – *OQ/Land Hessen* (Lūgums sniegt prejudiciālu nolēmumu – Fizisko personu aizsardzība attiecībā uz personas datu apstrādi – Regula (ES) 2016/679 – 22. pants – Automatizēts individuāls lēmums – Kredītinformācijas biroji – Automatizēta varbūtības vērtības iegūšana par personas spēju nākotnē pildīt maksājumu saistības ("*scoring*") – Šīs varbūtības vērtības izmantošana, ko veic trešā persona), <https://eur-lex.europa.eu/legal-content/LV/ALL/?uri=CELEX%3A62021CA0634>.

veidā²⁷. Automatizētas vecuma apstiprināšanas ietekme uz fizisko personu tiesībām var atšķirties atkarībā no attiecīgā pakalpojuma satura vai veida.

29. Tāpēc pakalpojumu sniedzējiem un visām trešām personām, kas iesaistītas vecuma apstiprināšanā, būtu jānodrošina tiesiskās aizsardzības līdzekļi un piemēroti tiesiskās aizsardzības mehānismi lietotājiem, kuru ar vecumu saistītie atribūti nav pienācīgi noteikti. Atkarībā no vecuma apstiprināšanas procesa struktūras pakalpojumu sniedzējiem un trešām personām ir jānorāda, ar ko datu subjektam būtu jāsažinās, lai īstenotu savas tiesības²⁸.
30. Pakalpojumu sniedzējiem un visām iesaistītajām trešām personām būtu jāpievērš īpaša uzmanība, ja runa ir par bērniem. Kā norādīts VDAR 71. apsvērumā, “tikai automatizēta apstrāde (..) kurai ir juridiskas sekas (..) vai kura līdzīgā veidā ievērojami ietekmē datu subjektu (..) nebūtu jāattiecinā uz bērnu”. Izņēmumi no šā noteikuma būtu jāsaģlabā ierobežotos apstākļos, piemēram, ja tas ir nepieciešams, “lai aizsargātu viņu labklājību”²⁹. Jebkurā gadījumā pakalpojumu sniedzējiem un visām iesaistītajām trešām personām būtu jāīsteno piemēroti pasākumi, piemēram, dzīvotspējīgas alternatīvas, tiesiskās aizsardzības mehānismi un – attiecīgā gadījumā – cilvēka līdzdalība nolūkā sniegt bērniem pielāgotu informāciju.

2.8 Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma

Vecuma apstiprināšanas sistēma būtu jāizstrādā, jāīsteno un jāizvērtē, ņemot vērā pieejamās metodes un tehnoloģijas, kas visvairāk aizsargā privātumu un tādējādi atbilst VDAR prasībām un efektīvi aizsargā datu subjektu tiesības.

31. Saskaņā ar VDAR 25. pantu datu pārziņiem, kas iesaistīti vecuma apstiprināšanā, būtu jāīsteno atbilstoši tehniskie un organizatoriskie pasākumi un nepieciešamie aizsardzības pasākumi, lai nodrošinātu visu datu aizsardzības principu un līdz ar to arī datu subjektu tiesību un brīvību efektīvu īstenošanu. Prasība pārziņiem pēc noklusējuma ņemt vērā datu aizsardzību jebkuras personas datu apstrādes darbības izstrādes posmā attiecas arī uz apstrādātājiem un visā apstrādes ciklā.
32. Ņemot vērā ar vecuma apstiprināšanas sistēmām saistīto risku daudzveidību un nopietnību, īpaši tad, kad tiek apstrādāti personu apliecinoši dokumenti vai īpašas personas datu kategorijas, piemēram, biometriskie dati, vislielākā uzmanība būtu jāpievērš tam, lai izvairītos no nevajadzīgas piekļuves personas datiem, to apstrādes, kopīgošanas un glabāšanas. Vecuma apstiprināšanas sistēmas un jebkurš juridisks vai tehnisks instruments, kurā noteiktas prasības šādām sistēmām, arī būtu regulāri jāpārskata un vajadzības gadījumā jāatjaunina, lai ņemtu vērā privātuma uzlabošanas tehnoloģiju strauji mainīgo vidi digitālās identitātes pārvaldības jomā.

²⁷ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 piemērošanas nolūkiem), <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁸ Kā norādīts iepriekš minētajās EDAK pamatnostādnēs: “Šīs tiesības ir pārsūdzamas pret pārzini, kas izveido profilu, un pārzini, kas pieņem automatizētu lēmumu par datu subjektu (ar cilvēka līdzdalību vai bez tās), ja šīs struktūras nav vienas un tās pašas”.

²⁹ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 piemērošanas nolūkiem): “Tomēr var būt daži apstākļi, kuros pārziņiem ir jāveic tikai automatizēta lēmumu pieņemšana, arī profilēšana, kas rada juridiskas vai līdzīgas būtiskas sekas attiecībā uz bērniem, piemēram, lai aizsargātu viņu labklājību”.

33. Kā minēts EDAK pamatnostādņēs par integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma³⁰, atsauce uz “tehnikas līmeni” VDAR 25. panta kontekstā uzliek datu pārziņiem pienākumu ņemt vērā pašreizējo tirgū pieejamo tehnoloģiju attīstību, kad tiek noteikti iepriekš minētie atbilstīgie tehniskie un organizatoriskie pasākumi. Minēto pasākumu noteikšanā var būt noderīgi standarti, paraugprakse un rīcības kodeksi, ko atzinušas attiecīgās ieinteresētās personas. Tomēr būtu jāpārbauda šo pasākumu piemērotība katrai konkrētajai apstrādes darbībai.
34. Attiecīgi EDAK, pamatojoties uz jaunākajiem sasniegumiem vecuma apstiprināšanas jomā šā dokumenta sagatavošanas laikā, iesaka pienācīgi ņemt vērā tehnoloģijas un arhitektūru, kas dod priekšroku lietotāju turētiem datiem un drošai vietējai apstrādei (balstītai uz ierīci) un ļauj izmantot tādas īpašības kā nesaistāmība³¹ (no dažādu pušu viedokļa un pat slepenu vienošanos vai datu aizsardzības pārkāpumu gadījumā) un selektīva personas datu izpaušana³², ko kontrolē datu subjekts. Turklāt gadījumos, kad vecuma apstiprināšana var radīt augstu risku datu subjektu privātumam, viņiem būtu jādara pieejamas metodes, kas balstās uz tādu pakešu izdošanu³³ kā vienreizlietojami akreditācijas dati vai kriptogrāfiski protokoli, piemēram, apliecinājums bez informācijas izpaušanas (*zero-knowledge*)³⁴.

2.9 Vecuma apstiprināšanas drošība

Pakalpojumu sniedzējiem un visām trešām personām, kas iesaistītas vecuma apstiprināšanā, būtu jāīsteno atbilstīgi tehniski un organizatoriski pasākumi, lai nodrošinātu riskam atbilstošu drošības līmeni.

35. Tādēļ VDAR ir prasība gan pārziņiem, gan apstrādātājiem ieviest atbilstošus tehniskus un organizatoriskus pasākumus, kuri nodrošina tādu drošības līmeni, kas atbilst riskam, ko rada personas datu apstrāde (83. apsvērums un 32. pants). Vecuma apstiprināšanā iesaistīto personas datu raksturs, sensitivitāte un apjoms norāda uz iespējamo nelabvēlīgo ietekmi, ko varētu radīt datu aizsardzības pārkāpums.
36. Uzticamības modeļi ir būtiski, lai novērstu datu aizsardzības pārkāpumus vecuma apstiprināšanas kontekstā, jo nosaka to, kā dažādas puses var verificēt cita citas identitāti un integritāti. Tie veicina drošu saziņu un datu apmaiņu starp dalībniekiem, kuriem, iespējams, iepriekš nav bijis nekādu attiecību. Turklāt personas datu pseidonimizācija un šifrēšana var būt noderīgi pasākumi, lai mazinātu datu aizsardzības pārkāpumu iespējamās nelabvēlīgās sekas. Glabāšanas ierobežojuma principa ievērošana un īsu glabāšanas periodu izmantošana var būt būtiska arī drošībai saistībā ar vecuma apstiprināšanu, jo samazina ietekmes tvērumu. Par vērtīgu aizsardzības pasākumu var uzskatīt politiku, kas neparedz žurnālu izmantošanu;

³⁰ EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (EDAK Pamatnostādnes 4/2019 par 25. pantu par integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma), versija 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 Nesaistāmības īpašība nozīmē, ka nav iespējams sasaistīt vai korelēt dažādus datu vienumus, darbības vai darījumus ar konkrētu datu subjektu.

³² Selektīva izpaušana ir marķierierīču, akreditācijas datu un apliecinājumu līdzeklis, kas katrā atsevišķā gadījumā datu subjektam dod iespēju ar konkrētām personām kopīgot tikai to informāciju, ko tie vēlas.

³³ Paketes izdošana ir atkarīga no tā, vai tiek atbildēts uz vienu datu subjekta apliecinājuma dokumentu pieprasījumu ar vienlaikus sagatavotu akreditācijas datu kopu vai grupu.

³⁴ “Zero-knowledge” pierādījums ir protokols, kurā viena puse (pierādītājs) var pierādīt otram pusei (verificētājam), ka kāds konkrēts apgalvojums ir patiess, nenododot verificētājam nekādu citu informāciju kā vienīgi to, ka šis apgalvojums ir patiess.

tas nozīmē, ka, kad ir pārbaudīts lietotāja vecums, vecuma apstiprināšanas procesā izmantotie personas dati netiek reģistrēti.

37. Ņemot vērā aizvien pieaugošo juridisko spiedienu īstenot vecuma apstiprināšanu un to pakalpojumu sniedzēju skaitu, uz kuriem var attiekties šādi noteikumi, praksē būtu jārēķinās ar drošības pārkāpumiem. Būtu jānoskaidro, vai ir ieviesti visi atbilstošie tehniskie un organizatoriskie pasākumi, lai varētu nekavējoties noteikt, vai ir noticis pārkāpums, un pēc tam noteikt, vai uz to attiecas paziņošanas pienākums³⁵. Jebkuras datu drošības politikas būtisks elements ir spēja, ja iespējams, novērst pārkāpumu un, ja tas notiek, savlaicīgi reaģēt. Tāpēc par būtisku būtu jāuzskata arī spēja nekavējoties atjaunot vecuma apstiprināšanas pieejamību pēc drošības pārkāpuma. Tāpat ir ļoti svarīgi nodrošināt vecuma apstiprināšanas ekosistēmas noturību, dodot priekšroku dažādām alternatīvām un brīvi saistītām pusēm³⁶, kas nav tik lielā mērā atkarīgas cita no citas, ka vienas sistēmas atteice vai sabrukums radītu būtiskus piekļuves ierobežojumus.
38. Lai gan drošības pasākumi ir ārkārtīgi svarīgi vecuma apstiprināšanā, tie negarantē, ka atļauta vai neatļauta piekļuve personas datiem neietekmēs fizisku personu tiesības. Tie nevar aizstāt nepieciešamības, samērīguma vai integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principu piemērošanu.

2.10 Pārskatbildība

Pakalpojumu sniedzējiem un visām iesaistītajām trešām personām būtu jāīsteno pārvaldības metodes, kas dod iespēju uzņemt atbildību par savu pieeju vecuma apstiprināšanai un par to, lai pierādītu atbilstību datu aizsardzības regulējumam un citām juridiskajām prasībām.

39. Ņemot vērā dažādu ieinteresēto personu iesaisti, vecuma apstiprināšanas pārvaldībai ir izšķiroša nozīme to pārskatbildībā. Vecuma apstiprināšanai būtu jādarbojas saskaņā ar pārvaldības sistēmu un jānodrošina, ka visi procesi un sistēmas tiek izstrādāti, īstenoti, pārskatīti, dokumentēti, novērtēti, izmantoti, uzturēti, testēti vai revidēti tā, lai tie atbilstu datu aizsardzības regulējumam un citām juridiskajām prasībām. Šajā satvarā būtu jāiekļauj vismaz datu aizsardzības politika (VDAR 24. panta 2. punkts) un prioritāšu noteikšanas un lēmumu pieņemšanas procesi, kas vajadzīgi, lai sasniegtu atbilstības mērķus un pienācīgi pārvaldītu riskus visā vecuma apstiprināšanas dzīves ciklā.
40. Piemēram, pārvaldības sistēmā būtu jānosaka, kas no pārziņa/apstrādātāja viedokļa ir atbildīgs un kādā veidā, un par kādām konkrētām darbībām vai darbībām apstrādes ietvaros. Tai būtu arī jānodrošina, ka iestādes un attiecīgās ieinteresētās personas var efektīvi revidēt vecuma apstiprināšanu. Pārvaldības sistēma ir būtiska ne tikai pārskatbildībai, bet arī pārredzamībai un uzticībai vecuma apstiprināšanas sistēmai. Datu subjekti biežāk uzticas metodēm, kas ir pārredzamas attiecībā uz to darbību, lēmumu pieņemšanu utt.

³⁵ EDPB Guidelines 9/2022 on personal data breach notification under GDPR (EDAK Pamatnostādnes 9/2022 par paziņošanu par personas datu aizsardzības pārkāpumiem saskaņā ar VDAR), https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

³⁶ Puses pēc iespējas mazāk ir atkarīgas cita no citas, ja tās samazina ietekmes tvērumu izmaiņu vai nepilnību gadījumā.

41. Turklāt daļa no pārvaldības sistēmas ietver vecuma apstiprināšanas efektivitātes nodrošināšanu (2.5. iedaļa), integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma (2.8. iedaļa) un drošību (2.9. iedaļa).

Eiropas Datu aizsardzības kolēģija

Priekšsēdētāja

(Anu Talus)