Statement

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

Pareiškimas Nr. 1/2025 dėl amžiaus užtikrinimo

Priimtas 2025 m. vasario 11 d.[1]

Europos duomenų apsaugos valdyba priėmė šį pareiškimą:

1. ŠIO PAREIŠKIMO APLINKYBĖS IR PASKIRTIS

1. ES reglamentavimo sistemoje raginama labiau apsaugoti vaikus skaitmeninėje aplinkoje. Pavyzdžiui, Audiovizualinės žiniasklaidos paslaugų direktyvoje[2], kurią valstybės narės perkėlė į savo nacionalinę teisę, pabrėžiama galimybė įgyvendinti amžiaus patikrinimo priemones (6a ir 28b straipsniai), BDAR nustatyti minimalaus amžiaus reikalavimai, taikomi norint duoti sutikimą, kad asmens duomenys būtų tvarkomi teikiant informacinės visuomenės paslaugas (8 straipsnis), Skaitmeninių paslaugų akte[3] amžiaus patikra minima kaip rizikos mažinimo priemonė (35 straipsnio 1 dalis), o kai kurios valstybės narės į savo nacionalinės teisės aktus yra įtraukusios minimalaus amžiaus reikalavimus, taikomus norint atlikti teisinius veiksmus, naudotis tam tikromis teisėmis arba gauti tam tikras prekes ir paslaugas.

2. Be to, pagal įvairias nacionalines ir Europos iniciatyvas, pavyzdžiui, Vaikams geresnio interneto strategiją (VGI+ strategiją) amžiaus užtikrinimas laikomas vienu iš sprendimų, kaip pagerinti vaikų gerovę internete sukuriant saugią ir pagal amžių pritaikytą skaitmeninę aplinką, atitinkančią Europos deklaraciją dėl skaitmeninių teisių ir principų[4].

[1] 2025 m. vasario 24 d. padaryti nedideli šio dokumento formato pataisymai. 2025 m. balandžio 1 d. padaryta papildomų nedidelių 16 ir 22 dalies b punkto pakeitimų.

[2] 2018 m. lapkričio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/1808, kuria, atsižvelgiant į kintančias rinkos realijas, iš dalies keičiama Direktyva 2010/13/ES dėl valstybių narių įstatymuose ir kituose teisės aktuose išdėstytų tam tikrų nuostatų, susijusių su audiovizualinės žiniasklaidos paslaugų teikimu, derinimo, (Audiovizualinės žiniasklaidos paslaugų direktyva), https://eur-lex.europa.eu/eli/dir/2018/1808/oj.

[3] 2022 m. spalio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2065 dėl bendrosios skaitmeninių paslaugų rinkos, kuriuo iš dalies keičiama Direktyva 2000/31/EB, (Skaitmeninių paslaugų aktas), https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

[4] Portalas „Better internet for kids“, Amžiaus užtikrinimo vadovas, https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest.

3. Remiantis tyrimo ataskaitoje *Amžiaus užtikrinimo tipologijų ir reikalavimų nustatymas*[5] pateikta apibrėžtimi, šiame dokumente terminas „amžiaus užtikrinimas“ bus vartojamas kaip *„bendrasis terminas kalbant apie metodus, kuriais įvairiu pasitikėjimo ar tikrumo lygiu nustatomas asmens amžius ar amžiaus intervalas“*. Toje pačioje ataskaitoje minimos trys pagrindinės amžiaus užtikrinimo kategorijos: amžiaus įvertinimas, amžiaus patikrinimas ir savideklaracija.
4. Amžiaus užtikrinimas kelia specifinių pavojų duomenų apsaugai ir gali neigiamai paveikti ne tik fizinių asmenų teisę į jų asmens duomenų apsaugą, bet ir kitas teises ir laisves[6], pavyzdžiui, teisę į nediskriminavimą, teisę į asmens neliečiamybę, teisę į laisvę ir saugumą, taip pat teisę į saviraiškos ir informacijos laisvę.

5. Pripažindama, koks svarbus nuoseklus požiūris į amžiaus užtikrinimą ES lygmeniu, Europos duomenų apsaugos valdyba (toliau – EDAV) nori pateikti konkrečias gaires ir iš BDAR kylančius aukšto lygio principus, į kuriuos reikėtų atsižvelgti tvarkant asmens duomenis amžiaus užtikrinimo aplinkybėmis.

6. Siūlomais principais siekiama suderinti vaikų apsaugą ir asmens duomenų apsaugą amžiaus užtikrinimo aplinkybėmis.

7. Pirmenybė teikiama reikalavimams, susijusiems su pagrindiniais BDAR 5 straipsnyje nustatytais principais (teisėtumu, sąžiningumu, skaidrumu, tikslo apribojimu, duomenų kiekio mažinimu, tikslumu, saugojimo trukmės apribojimu, konfidencialumu, vientisumu ir atskaitomybe), ir siekiui užtikrinti, kad šie duomenų apsaugos principai būtų tinkamai įgyvendinami ir ilgainiui išliktų patikimi, kaip nustatyta BDAR 25 straipsnyje „Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga“ ir BDAR 32 straipsnyje „Duomenų tvarkymo saugumas“.

8. Šiame pareiškime daugiausia dėmesio skiriama principams, taikomiems įvairiems internetinio naudojimo atvejams, įskaitant tokius, kai, norint įsigyti produktus, naudotis paslaugomis, kurios gali pakenkti vaikams, arba atlikti teisinius veiksmus, teisės aktais ar kitais būdais nustatytas minimalus amžius, taip pat kai esama pareigos rūpintis vaikais (pavyzdžiui, užtikrinti, kad paslaugos būtų kuriamos arba siūlomos atsižvelgiant į amžių).

9. EDAV taip pat gali apsvarstyti galimybę prireikus ir kituose dokumentuose pateikti papildomų gairių dėl konkrečių naudojimo atvejų.

[5] Raiz Shaffique, M., & van der Hof, S. (2024). Amžiaus užtikrinimo tipologijų ir reikalavimų nustatymas. Tyrimo ataskaita, Europos mokyklų tinklo koordinuojamo ir Europos Komisijos užsakyto projekto „Better internet for kids“ dalis.

[6] Apie galimą amžiaus užtikrinimo poveikį teisėms ir laisvėms žr., pvz.: „Roadmap for age verification“ (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“ (AEPD, 2024), https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf arba „Trustworthy Age Assurance?“, Verts/ALE Žaliosios ir socialinės ekonomikos klasterio Europos Parlamente užsakytas tyrimas (2024), https://www.greens-efa.eu/lt/article/document/trustworthy-age-assurance.

2. BDAR REIKALAVIMUS ATITINKANČIO AMŽIAUS UŽTIKRINIMO PRINCIPAI

2.1 Visapusiškas ir veiksmingas naudojimasis teisėmis ir laisvėmis

Amžiaus užtikrinimas turi neprieštarauti visam fizinių asmenų pagrindinių teisių ir laisvių rinkiniui[7], o visos procese dalyvaujančios šalys pirmiausia turėtų atsižvelgti į geriausius vaiko interesus.

10. Įgyvendindami amžiaus užtikrinimą, paslaugų teikėjai turėtų būtinai atsižvelgti ne tik į poveikį teisei į asmens duomenų apsaugą, bet ir į visas fizinių asmenų pagrindines teises.

11. Konkrečiu vaikų atveju visos su amžiaus užtikrinimu susijusios šalys pirmiausia turėtų atsižvelgti į geriausius vaiko interesus[8]. Svarbu pažymėti, kad vertinant geriausius vaiko interesus nėra hierarchijos ir reikėtų atsižvelgti į visas vaikų teises[9], įskaitant jų teisę į asmens duomenų apsaugą, apsaugą nuo smurto ir visų kitų išnaudojimo formų, kad jie galėtų susipažinti su informacija iš įvairių šaltinių ir būtų deramai atsižvelgiama į jų nuomonę.

2.2 Rizika grindžiamas amžiaus užtikrinimo proporcingumo vertinimas

Amžiaus užtikrinimas visada turėtų būti įgyvendinamas rizika grindžiamu ir proporcingu būdu, suderinamu su fizinių asmenų teisėmis ir laisvėmis.

12. Paslaugų teikėjai, rengdami ir teikdami savo paslaugas, turėtų laikytis rizika grindžiamo požiūrio. Atsižvelgiant į susijusią riziką, turėtų būti įrodytas saugos priemonių, pvz., amžiaus užtikrinimo, naudojimo būtinumas ir proporcingumas. Būtinumą būtų galima įrodyti atliekant vertinimą[10], taip siekiant nustatyti ir įvertinti riziką, kurią tam tikra paslauga kelia vaikams[11], pavyzdžiui, žalingo kontakto ar turinio poveikio riziką. Atlikdami šį vertinimą paslaugų teikėjai taip pat gali atsižvelgti į vaikų teises, skaitmeninės aplinkos teikiamas galimybes, vaikų nuomonę ir besiformuojančius jų gebėjimus, kad būtų užtikrintas pagal amžių tinkamas dalyvavimas[12].

13. Paslaugų teikėjai taip pat turi gerbti savo naudotojų teises ir laisves, įskaitant teisę į jų asmens duomenų apsaugą, derindami šias teises ir laisves su poreikiu imtis saugos priemonių, kurios visada turėtų būti mažiausiai privatumą pažeidžiančios iš visų galimų ir kurios visada turėtų būti veiksmingos. Daugeliu atvejų amžiaus užtikrinimas kelia didelį pavojų duomenų subjektų teisėms ir laisvėms, todėl prieš tvarkant duomenis, atsižvelgiant į duomenų tvarkymo pobūdį,

---

[7] Visų pirma Visuotinei žmogaus teisių deklaracijai, Europos žmogaus teisių konvencijai, Europos Sąjungos pagrindinių teisių chartijai ir JT vaiko teisių konvencijai.

[8] JT Vaiko teisių komitetas paaiškino, kad geriausių vaiko interesų principu „siekiama užtikrinti visapusišką ir veiksmingą naudojimąsi visomis Konvencijoje pripažintomis teisėmis ir visapusišką vaiko raidą“. Bendroji pastaba Nr. 14 (2013) dėl vaiko teisės į tai, kad pirmiausia būtų vadovaujamasi jo interesu (3 straipsnio 1 dalis), https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.

[9] Bendroji pastaba Nr. 25 (2021) dėl vaikų teisių, susijusių su skaitmenine aplinka, OHCHR, 2021 m. kovo mėn.

[10] Pavyzdžiui, poveikio vaiko teisėms vertinimą, kuris gali būti įtrauktas arba neįtrauktas į poveikio duomenų apsaugai vertinimą (PDAV).

[11] Vaiko teisių srities ekspertai pabrėžė, kad poveikio vaiko teisėms vertinimus naudinga naudoti kaip veiksmingą priemonę „[Vaiko teisių] konvencijai ir jos 3 straipsniui praktiškai įgyvendinti, konkrečiai ir struktūriškai teikiant pirmenybę geriausiems vaiko interesams“ (in Mukherjee, S., Pothong, K., & Livingstone, S. (2021). Child Rights Impact Assessment: A tool to realise child rights in the digital environment. London: 5Rights Foundation). Be to, JT komitetas paragino valstybes įgalioti taikyti poveikio vaiko teisėms vertinimą, kad vaikų teisės būtų įtrauktos į skaitmeninės aplinkos reguliavimą ir kūrimą.

[12] Bendroji pastaba Nr. 25 (2021) dėl vaikų teisių, susijusių su skaitmenine aplinka, OHCHR, 2021 m. kovo mėn.

aprėptį, kontekstą ir tikslus, reikėtų atlikti poveikio duomenų apsaugai vertinimą (toliau – PDAV, BDAR 35 straipsnis). PDAV turėtų apimti sistemingą numatytų duomenų tvarkymo operacijų aprašymą ir duomenų tvarkymo tikslus, įskaitant, kai taikytina, teisėtus interesus, kurių siekia duomenų valdytojas. Poveikio duomenų apsaugai vertinime taip pat turėtų būti išdėstytas duomenų tvarkymo būtinumo ir proporcingumo vertinimas, nustatyta rizika, kylanti dėl asmens duomenų tvarkymo amžiaus užtikrinimo tikslais, ir numatytos tos rizikos mažinimo priemonės[13].

14. PDAV turėtų būti vadovaujamasi rengiant ir įgyvendinant tinkamas technines ir organizacines duomenų apsaugos reikalavimų laikymosi priemones. Šis rizika grindžiamas požiūris yra itin svarbus derinant galimą kišimąsi į fizinių asmenų teises bei laisves ir šiomis konkrečiomis aplinkybėmis siekiamą tikslą, t. y. vaikų saugumą. Visada būtina atidžiai įvertinti šio kišimosi sritį, mastą ir intensyvumą, kiek tai susiję su poveikiu teisėms ir laisvėms[14]. Pavyzdžiui, paslaugų teikėjas, tvarkantis asmens duomenis, kad patikrintų visų savo naudotojų amžių, kai jie prisijungia prie viso paslaugų teikėjo turinio ar paslaugų, net jei turinys ar paslaugos tinka bet kokiai auditorijai ir nekelia jokios rizikos, neatitiktų būtinumo ir proporcingumo kriterijų.

2.3 Duomenų apsaugai kylančios rizikos prevencija

Amžiaus užtikrinimas neturėtų kelti nereikalingos rizikos fizinių asmenų duomenų apsaugai. Visų pirma amžiaus užtikrinimas neturėtų suteikti paslaugų teikėjams papildomų priemonių fiziniams asmenims identifikuoti, jų buvimo vietai nustatyti, juos profiliuoti ar sekti.

15. Paslaugų teikėjai ir visos su amžiaus užtikrinimu susijusios trečiosios šalys turėtų įgyvendinti veiksmingas priemones ir apsaugos priemones, kad šis procesas nekeltų nereikalingos rizikos duomenų apsaugai, pavyzdžiui, atsirandančios dėl fizinių asmenų identifikavimo, jų buvimo vietos nustatymo, profiliavimo ar sekimo. Asmens duomenų tvarkymas amžiaus užtikrinimo tikslais neturėtų suteikti papildomų priemonių tikslams, nesusijusiems su pačiu amžiaus užtikrinimu, pasiekti. Tam reikia pasirinkti amžiaus užtikrinimo metodus, kurie visiškai atitiktų pritaikytosios ir standartizuotosios duomenų apsaugos principą (žr. 2.8 skirsnį), ir įgyvendinimo priemones, kuriomis būtų garantuojamas sąžiningumo principas ir būtų užtikrinama, kad asmens duomenys nebūtų tvarkomi duomenų subjektams nepagrįstais, žalingais, neteisėtai juos diskriminuojančiais, netikėtais ar klaidinančiais būdais.

16. Pavyzdžiui, fizinis asmuo, kuris turi leisti patikrinti jo amžių, kad galėtų susipažinti su suaugusiųjų turiniu, nesitikėtų, kad paslaugų teikėjas amžiaus užtikrinimu naudosis siekdamas nustatyti asmens tapatybę ar tikslią geografinę vietą arba stebėti, vertinti ar daryti išvadas apie asmeninius to asmens tapatybės aspektus. Tai ypač svarbu siekiant laikytis BDAR 5 straipsnio 1 dalyje nustatytų duomenų apsaugos principų, įskaitant sąžiningumą, skaidrumą ir tikslo apribojimą, ir 6 straipsnio 4 dalyje nustatytų taisyklių, susijusių su tolesniu asmens duomenų naudojimu. Panašiai, laikantis BDAR 5 straipsnio 1 dalyje nustatytų tikslo apribojimo ir duomenų kiekio mažinimo principų, amžiaus užtikrinimo procesas neturėtų sudaryti sąlygų toliau tikslingai kreiptis į naudotojus ar juos profiliuoti, be kita ko, tiek komercinio (pvz.,

[13] EDAV Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento (ES) 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų, https://ec.europa.eu/newsroom/article29/items/611236/lt.
[14] EDAPP gairės dėl priemonių, kuriomis apribojamos pagrindinės teisės į privatumą ir asmens duomenų apsaugą, proporcingumo vertinimo, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

individualizuotos reklamos), tiek piktavališko atrankiojo adresavimo (pvz., viliojimo, tyčiojimosi, persekiojimo ar priekabiavimo) tikslais. EDAV primena, kad pagal BDAR 75 konstatuojamąją dalį duomenų apsaugos teisėms gali kilti ypatingas pavojus, kai asmens duomenys yra susiję su pažeidžiamais fiziniais asmenimis, visų pirma vaikais. Apskritai neturėtų būti įmanoma daugiau nei būtina sužinoti apie fizinį asmenį ir jo veiksmus profiliuojant šį asmenį pagal amžiaus užtikrinimo procese naudojamą informaciją. Ši nuostata turėtų būti kuo labiau užtikrinta ir duomenų saugumo pažeidimo atveju.

17. Turėtų būti vengiama situacijų, susijusių su galios disbalansu, kad paslaugų teikėjai neverstų asmenų patirti nereikalingos rizikos duomenų apsaugai dėl to, kad jie nepakankamai nusimano[15]. Kai tai nėra įmanoma, šie atvejai turėtų būti pripažįstami ir į juos turėtų būti atsižvelgiama taikant tinkamas atsakomąsias priemones[16]. Pavyzdžiui, naudotojams, kurie negali arba nenori taikyti konkretaus amžiaus užtikrinimo metodo, turėtų būti suteiktos kitos tinkamos alternatyvos jų amžiui įrodyti. Be to, paslaugų teikėjai turėtų reguliariai vertinti, ar pasirinkti metodai ir technologijos, įskaitant trečiųjų šalių pateiktus metodus ir technologijas, veikia pagal jų tikslus, ir juos pritaikyti, kad būtų užtikrintas teisingas duomenų tvarkymas. Amžiaus užtikrinimo procese dalyvaujančios trečiosios šalys taip pat turėtų siekti padėti paslaugų teikėjams laikytis įsipareigojimų, nekeldamos nereikalingos rizikos duomenų apsaugai ir laiku pranešdamos apie visus svarbius savo politikos, dizaino, paslaugų ir kt. pakeitimus.

2.4 Tikslo apribojimas ir duomenų kiekio mažinimas

Paslaugų teikėjai ir bet kuri trečioji šalis, dalyvaujanti amžiaus užtikrinimo procese, turėtų tvarkyti informaciją tik apie tuos su amžiumi susijusius požymius, kurie yra tikrai būtini nustatytam, aiškiai apibrėžtam ir teisėtam jų tikslui pasiekti.

18. Dažniausiai amžiaus užtikrinimo tikslas – priimti su amžiumi susijusius prieigos kontrolės sprendimus, užkirsti kelią žalai internete vaikams, pasiūlyti tinkamą dizainą ar patirtį pagal amžių ir pan. Neatsižvelgiant į naudojimo atvejį, asmens duomenų tvarkymo tikslas turėtų būti konkretus ir aiškus (BDAR 5 straipsnio 1 dalies b punktas). Surinkus asmens duomenis, jie negali būti toliau tvarkomi ar derinami su papildomais duomenimis tokiu būdu, kuris būtų nesuderinamas su tais tikslais. Siekiant apriboti galimybę pakeisti asmens duomenų naudojimo tikslą, turėtų būti taikomos tokios techninės priemonės kaip privatumo didinimo technologijos. Taip pat turėtų būti taikomos organizacinės priemonės, pavyzdžiui, politikos priemonės ir sutartiniai įsipareigojimai, kuriais ribojamas pakartotinis asmens duomenų naudojimas[17].

19. Su amžiumi susijęs požymis – tai bet koks požymis, rodantis, kad fizinis asmuo yra tam tikro amžiaus, vyresnis ar jaunesnis nei tam tikro amžiaus arba priklauso tam tikrai amžiaus grupei.

[15] Pavyzdžiui, kai su duomenų subjektais susiję sprendimai priimami automatizuotai, netaikant tinkamų teisių gynimo mechanizmų, arba kai sutikimo negalima duoti laisva valia. „Galios disbalanso“ sąvoka aptariama EDAV nuomonėje 08/2024 dėl galiojančio sutikimo, duodamo pagal modelius „sutik arba mokėk“, įdiegtus didelėse interneto platformose (4.2.1.3 skirsnis), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_lt.pdf.

[16] Iš EDAV gairių Nr. 03/2022 dėl manipuliatyvių dizaino sprendimų socialinės žiniasklaidos platformose: kaip juos atpažinti ir jų išvengti (2.3 skirsnis), 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.

[17] Iš EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“, Versija 2.0, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_lt.pdf.

Aktualius ir būtinus su amžiumi susijusius požymius, apie kuriuos reikia surinkti informaciją, lemia nurodytas tikslas. Tai padaręs duomenų valdytojas taip pat galės įvertinti amžiaus užtikrinimo proceso proporcingumą. Šio proceso teikiamos naudos neturėtų nusverti jokie nepalankūs aspektai, susiję su naudojimusi pagrindinėmis teisėmis[18] (žr. 2.2 skirsnį).

20. Todėl duomenų valdytojas turėtų rinkti tik tuos asmens duomenis, kurie yra būtini, tinkami ir susiję su tikslais, kuriuos ketinama pasiekti. Taip duomenų kiekio mažinimas padeda pagrįsti ir įgyvendinti būtinumo[19] ir proporcingumo principus. Pavyzdžiui, paslaugų teikėjui gali reikėti tik žinoti, ar naudotojas yra vyresnis ar jaunesnis už tam tikrą amžiaus ribą. Tai būtų galima įgyvendinti taikant prieigos rakto metodą, grindžiamą paslaugas teikiančios trečiosios šalies dalyvavimu, kai paslaugų teikėjas mato tik funkcinį amžiaus užtikrinimo proceso rezultatą (pvz., ar asmuo yra vyresnis, ar jaunesnis už tam tikrą amžiaus ribą)[20]. Gali būti aktualūs skirtingi metodai, kai paslaugų teikėjui reikia žinoti, ar naudotojas priklauso tam tikrai amžiaus grupei, ar gimė konkrečiais metais.

2.5 Amžiaus užtikrinimo veiksmingumas

Amžiaus užtikrinimas turėtų akivaizdžiai pasiekti tokį veiksmingumo lygį, kuris atitiktų tikslą, dėl kurio jis atliekamas.

21. Priemonės, kuriomis atliekamas amžiaus užtikrinimas, turėtų būti tinkamos duomenų tvarkymo tikslui pasiekti. Visų pirma bet kurios teisiškai privalomos amžiaus užtikrinimo priemonės veiksmingumas turėtų būti laikomas būtinumo[21] ir proporcingumo[22] principų laikymosi išankstine sąlyga.

22. Amžiaus užtikrinimo veiksmingumas turėtų būti vertinamas keliais aspektais, įskaitant nurodytus toliau.

a) Prieinamumas. Fiziniams asmenims turėtų būti plačiai prieinama amžiaus užtikrinimo funkcija, kad jie galėtų patvirtinti savo amžių arba įrodyti, kad atitinka su amžiumi susijusį reikalavimą. Kai kyla pavojus, kad tam tikrų kategorijų asmenys gali būti diskriminuojami taikant konkretų amžiaus užtikrinimo metodą, pavyzdžiui, dėl to, kad jie neturi tinkamo tapatybės dokumento ar mobiliojo telefono, arba dėl negalios, turėtų būti numatyti alternatyvūs amžiaus užtikrinimo metodai, kai pagrįstai įmanoma, pasirūpinant tinkamu privatumo, saugos ir saugumo lygiu. Amžiaus užtikrinimo sprendimai taip pat turėtų atitikti visus taikytinus teisės aktus dėl prieinamumo[23].

[18] Iš EDAPP gairių dėl priemonių, kuriomis ribojamos pagrindinės teisės į privatų gyvenimą ir asmens duomenų apsaugą, proporcingumo vertinimo, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[19] Iš EDAPP priemonių rinkinio dėl priemonių, kuriomis ribojama pagrindinė teisė į asmens duomenų apsaugą, būtinumo vertinimo, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

[20] Paslaugas teikianti trečioji šalis atlieka amžiaus patikrą ir suteikia naudotojui vadinamąjį amžiaus raktą, kurį naudotojas gali pateikti paslaugų teikėjui neprivalėdamas dar kartą įrodyti savo amžiaus. Amžiaus raktas gali turėti skirtingų naudotojo požymių ir informacijos apie tai, kada, kur ir kaip buvo atlikta amžiaus patikra.

[21] EDAPP priemonių rinkinys dėl priemonių, kuriomis ribojama pagrindinė teisė į asmens duomenų apsaugą, būtinumo vertinimo, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

[22] Gairės dėl priemonių, kuriomis apribojamos pagrindinės teisės į privatumą ir asmens duomenų apsaugą, proporcingumo vertinimo, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[23] Pavyzdžiui, viešojo sektoriaus interneto svetainių ir mobiliųjų programų prieinamumas ir gaminių bei paslaugų prieinamumas numatyti atitinkamai Interneto svetainių prieinamumo direktyvoje ir Europos prieinamumo akte (EPA). Turi būti pasirūpinta, kad amžiaus užtikrinimo

b) Patikimumas. Pagal tikslumo principą (BDAR 5 straipsnio 1 dalies d punktas) bet koks metodas, kuriuo siekiama nustatyti, ar fizinis asmuo atitinka su amžiumi susijusį reikalavimą, turėtų užtikrinti tinkamą ir nuoseklų tikslumo lygį nustatant, ar asmuo atitinka minėtą reikalavimą. Turėtų būti numatyti tinkami teisių gynimo mechanizmai, ypač tais atvejais, kai automatizuotas sprendimų priėmimas gali daryti didelį poveikį naudotojams, pavyzdžiui, kai nėra tinkamai nustatyti jų su amžiumi susiję požymiai (žr. 2.7 skirsnį).
c) Atsparumas. Amžiaus užtikrinimo priemonėmis turėtų būti įmanoma reaguoti į nenumatytas situacijas ir atlaikyti pagrįstai tikėtinus bandymus apgauti ar apeiti sistemą. Reikėtų pažymėti, kad atsparumas beveik neturi prasmės taikant su amžiumi susijusio požymio savideklaraciją, nes tokio metodo patikimumas daugiausia priklauso nuo naudotojo geros valios[24].

Be to, amžiaus užtikrinimą įgyvendinantys paslaugų teikėjai ir visos procese dalyvaujančios trečiosios šalys turėtų sugebėti įrodyti amžiaus užtikrinimo veiksmingumą ir skaidriai nurodyti priemones, kuriomis jie pasiekia tinkamą prieinamumo, patikimumo ir atsparumo lygį (žr. 2.10 skirsnį).

2.6 Teisėtumas, sąžiningumas ir skaidrumas

Paslaugų teikėjai ir visos amžiaus užtikrinimo procese dalyvaujančios trečiosios šalys turėtų užtikrinti, kad bet kokių asmens duomenų tvarkymas amžiaus užtikrinimo tikslais būtų teisėtas, sąžiningas ir skaidrus naudotojams.

23. Paslaugų teikėjai turi užtikrinti, kad jie turėtų taikytiną teisinį pagrindą pagal BDAR 6 straipsnį (ir, jei aktualu, taikytiną 9 straipsnio 2 dalyje nustatytą išimtį) asmens duomenims tvarkyti, kiek tai susiję su amžiaus užtikrinimu. Pavyzdžiui, jiems gali reikėti įdiegti amžiaus užtikrinimo funkciją, kad būtų įvykdyta teisinė prievolė (BDAR 6 straipsnio 1 dalies c punktas), atsižvelgiant į tai, kad amžiaus užtikrinimas turi būti proporcingas siekiamam teisėtam tikslui ir BDAR 6 straipsnio 3 dalyje nustatytiems reikalavimams.

24. Be to, paslaugų teikėjai turi skaidriai informuoti naudotojus apie tai, kaip tiksliai ir kas naudoja jų asmens duomenis. Tai ypač svarbu, kai amžiaus užtikrinimo procese dalyvauja daug šalių. Prieš amžiaus užtikrinimo tikslais tvarkant bet kokius asmens duomenis, naudotojai turi būti informuojami (pagal BDAR 12, 13 ir 14 straipsnius), be kita ko, apie šiuos aspektus[25]:

- kokie asmens duomenys bus tvarkomi ir kaip;
- ar procese dalyvaus trečiosios šalys ir, jei taip, kas jos yra ir kas yra duomenų valdytojai ir duomenų tvarkytojai šiame scenarijuje;
- ar jų duomenimis bus dalijamasi su kitais arba jie bus perduoti trečiajai šaliai;

sprendimai būtų suderinti su šiais teisės aktais ir atitiktų darniojo Europos standarto „IRT produktų ir paslaugų prieinamumo reikalavimai“, EN 301 549 v3.2.1, reikalavimus.

[24] EDAV jau yra išreiškusi rimtų abejonių dėl savideklaracijos, kaip amžiaus tikrinimo metodo, veiksmingumo vykdant didelės rizikos duomenų tvarkymą – Privalomas sprendimas Nr. 2/2023 dėl Airijos priežiūros institucijos pateikto skundo dėl įmonės „TikTok Technology Limited“ (BDAR 65 straipsnis), https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf.

[25] Žr. 29 straipsnio darbo grupės Skaidrumo užtikrinimo pagal Reglamentą 2016/679 gaires, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_lt.pdf.

- kiek laiko bus saugomi jų asmens duomenys arba, jei tai neįmanoma, kokie yra saugojimo laikotarpio nustatymo kriterijai;
- kokios yra jų teisės, susijusios su jų asmens duomenimis (BDAR 15–22 straipsniai), įskaitant tai, kaip jie gali ginčyti neteisingą sprendimą, priimtą dėl amžiaus užtikrinimo.

25. Skaidrumas amžiaus užtikrinimo srityje yra ypač svarbus kalbant apie vaikus. Paslaugų teikėjai turi užtikrinti, kad su tuo susijusi informacija apie skaidrumą vaikams būtų perteikiama aiškiai ir jiems lengvai suprantamai.

26. Skaidrumo sąvoka iš esmės susijusi su sąžiningumu. Jei paslaugų teikėjai aiškiai ir skaidriai neinformuoja apie tai, kaip jie tvarko fizinių asmenų informaciją amžiaus užtikrinimo tikslais, mažai tikėtina, kad toks duomenų tvarkymas gali būti laikomas sąžiningu, todėl mažai tikėtina, kad toks duomenų tvarkymas yra teisėtas. Visų pirma, jei paslaugų teikėjas naudotojams siūlo skirtingus savo amžiaus tikrinimo metodus, jis turėtų skaidriai nurodyti kiekvieno metodo poveikį duomenų apsaugos požiūriu.

2.7 Automatizuotas sprendimų priėmimas

Bet kokie automatizuoto sprendimų priėmimo atvejai, susiję su amžiaus užtikrinimu, turėtų atitikti BDAR. Jei taikytina, paslaugų teikėjai ir visos susijusios trečiosios šalys turėtų numatyti tinkamas priemones fizinių asmenų teisėms ir laisvėms bei teisėtiems interesams apsaugoti.

27. ES teisės aktų leidėjas pasirinko plačią automatizuoto sprendimų priėmimo apibrėžtį, kurią reikia nagrinėti kiekvienu konkrečiu atveju[26]. Automatizuoti sprendimai gali būti priimami įvairiais amžiaus užtikrinimo proceso etapais, siekiant gauti prieigą prie turinio ar paslaugos arba taikant amžiaus įrodymo metodus.

28. Visiškai automatizuotas amžiaus užtikrinimas gali turėti teisinių pasekmių atitinkamiems fiziniams asmenims, pavyzdžiui, jų naudojimuisi saviraiškos laisve, arba bent jau gali daryti jiems didelį panašų poveikį[27]. Automatizuoto amžiaus užtikrinimo poveikis fizinių asmenų teisėms gali skirtis priklausomai nuo atitinkamo turinio ar paslaugų rūšies.

29. Todėl paslaugų teikėjai ir visos amžiaus užtikrinimo procese dalyvaujančios trečiosios šalys turėtų numatyti teisių gynimo priemones ir tinkamus teisių gynimo mechanizmus naudotojams, kurių su amžiumi susiję požymiai nenustatomi tinkamai. Priklausomai nuo amžiaus užtikrinimo proceso struktūros, šie amžiaus užtikrinimo proceso dalyviai turi nurodyti, į ką duomenų subjektas turėtų kreiptis, kad galėtų pasinaudoti savo teisėmis[28].

---

[26] Byla C-634/21, *SCHUFA Holding (Scoring)*: 2023 m. gruodžio 7 d. Teisingumo Teismo (pirmoji kolegija) sprendimas byloje (*Verwaltungsgericht Wiesbaden* (Vokietija) prašymas priimti prejudicinį sprendimą) *OQ / Land Hessen* (*Prašymas priimti prejudicinį sprendimą – Fizinių asmenų apsauga tvarkant asmens duomenis – Reglamentas (ES) 2016/679 – 22 straipsnis – Automatizuotas atskiras sprendimas – Komercinę informaciją teikiančios bendrovės – Automatizuotas tikimybės rodiklio, susijusio su asmens pajėgumu ateityje įvykdyti mokėjimo įsipareigojimus, nustatymas (scoring) – Trečiųjų šalių naudojimasis šiuo tikimybės rodikliu*), https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX%3A62021CA0634.

[27] Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės, https://ec.europa.eu/newsroom/article29/items/612053/lt.

[28] Kaip nurodyta EDAV gairėse (pirmiau minėtose): „*šiomis teisėmis galima pasinaudoti profilį sudarančio duomenų valdytojo ir, jei tai nėra tas pats subjektas, automatizuotą sprendimą (su žmogaus įsikišimu ar be jo) dėl duomenų subjekto priimančio valdytojo atžvilgiu*“.

30. Kalbant apie vaikus, paslaugų teikėjai ir bet kuri susijusi trečioji šalis turėtų veikti itin dėmesingai. Kaip nurodyta BDAR 71 konstatuojamojoje dalyje, „*priemonė, <...> grindžiama tik automatizuotu duomenų tvarkymu, <...> kuri <...> turi teisinių pasekmių arba <...> daro panašų didelį poveikį*, *<...> negali būti susijusi su vaiku*“. Šios taisyklės išimtys ir toliau turėtų būti taikomos ribotomis aplinkybėmis, pavyzdžiui, kai „*reikia apsaugoti jų gerovę*“[29]. Bet kuriuo atveju paslaugų teikėjai ir bet kuri susijusi trečioji šalis turėtų įgyvendinti tinkamas priemones, pvz., kitas tinkamas alternatyvas, teisių gynimo mechanizmus ir, kai taikytina, žmogaus įsikišimą, teikiant vaikams pritaikytą informaciją, kai tai aktualu.

2.8 Pritaikytoji ir standartizuotoji duomenų apsauga

Siekiant laikytis BDAR reikalavimų ir veiksmingai apsaugoti duomenų subjektų teises, amžiaus užtikrinimas turėtų būti kuriamas, įgyvendinamas ir vertinamas atsižvelgiant į labiausiai privatumą saugančius prieinamus metodus ir technologijas.

31. Pagal BDAR 25 straipsnį duomenų valdytojai, dalyvaujantys amžiaus užtikrinimo procese, turėtų įgyvendinti tinkamas technines ir organizacines priemones ir būtinas apsaugos priemones, kad užtikrintų veiksmingą visų duomenų apsaugos principų ir atitinkamai duomenų subjektų teisių ir laisvių įgyvendinimą. Reikalavimas, kad duomenų valdytojai standartiškai atsižvelgtų į duomenų apsaugą bet kokios asmens duomenų tvarkymo veiklos projektavimo etape, taip pat taikomas duomenų tvarkytojams ir galioja per visą duomenų tvarkymo gyvavimo ciklą.

32. Atsižvelgiant į rizikos, susijusios su amžiaus užtikrinimo sistemomis, įvairovę ir rimtumą, ypač kai tvarkomi tapatybės dokumentai ar specialių kategorijų asmens duomenys, pavyzdžiui, biometriniai duomenys, reikėtų ypač daug dėmesio skirti tam, kad būtų išvengta nereikalingos prieigos prie asmens duomenų, jų tvarkymo, dalijimosi jais ir jų saugojimo. Amžiaus užtikrinimo sistemos ir visos teisinės ar techninės priemonės, kuriomis nustatomi tokių sistemų reikalavimai, taip pat turėtų būti reguliariai peržiūrimos ir prireikus atnaujinamos, kad būtų atsižvelgta į sparčiai kintančią privatumo didinimo technologijų aplinką skaitmeninės tapatybės valdymo srityje.

33. Kaip nurodyta EDAV gairėse dėl pritaikytosios ir standartizuotosios duomenų apsaugos[30], BDAR 25 straipsnyje nurodyta prievolė atsižvelgti į „techninių galimybių išsivystymo lygį“ įpareigoja duomenų valdytojus, nustatant minėtąsias tinkamas technines ir organizacines priemones, atsižvelgti į dabartinę rinkoje esamų technologijų pažangą. Nustatant tokias priemones gali būti naudingi standartai, geriausia praktika ir elgesio kodeksai, kuriuos pripažįsta atitinkami suinteresuotieji subjektai. Tačiau reikėtų patikrinti, ar šios priemonės yra tinkamos kiekvienai konkrečiai duomenų tvarkymo veiklai.

34. Todėl, remdamasi šio dokumento parengimo metu turima naujausia informacija apie amžiaus užtikrinimą, EDAV rekomenduoja tinkamai atsižvelgti į technologijas ir struktūras, kuriomis sudaromos palankesnės sąlygos naudotojų saugomiems duomenims ir saugiam duomenų

[29] Iš Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą (ES) 2016/679 gairių: „*Tačiau gali būti aplinkybių, kai duomenų valdytojams būtina vaikų atžvilgiu taikyti automatizuotą sprendimų priėmimą, įskaitant profiliavimą, dėl kurio kyla teisinių pasekmių arba panašiu būdu daromas didelis poveikis, pvz., kai reikia apsaugoti jų gerovę*“.

[30] EDAV gairės 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“, Versija 2.0, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_lt.pdf.

tvarkymui vietoje (įrenginyje), sudarant sąlygas tokioms ypatybėms kaip nesusiejimas[31] (įvairių šalių požiūriu ir net procesų apėjimo ar duomenų saugumo pažeidimų atveju) ir pasirinktinis duomenų subjekto valdomų asmens duomenų atskleidimas[32]. Be to, tais atvejais, kai amžiaus užtikrinimas gali kelti didelę riziką duomenų subjektų privatumui, duomenų subjektams turėtų būti suteikta galimybė naudotis tokiais metodais kaip vienkartinių kredencialų išdavimas partijomis[33] arba kriptografiniai protokolai, pvz., nulinio žinojimo protokolas[34].

2.9 Amžiaus užtikrinimo saugumas

Paslaugų teikėjai ir visos amžiaus užtikrinimo procese dalyvaujančios trečiosios šalys turėtų įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas riziką atitinkantis saugumo lygis.

35. BDAR reikalaujama, kad duomenų valdytojai ir duomenų tvarkytojai įgyvendintų tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų tvarkomiems asmens duomenims atitinkančio lygio saugumas (83 konstatuojamoji dalis ir 32 straipsnis). Asmens duomenų, kurie gali būti įtraukti į amžiaus užtikrinimą, pobūdis, jautrumas ir apimtis rodo galimą neigiamą poveikį, kurį galėtų sukelti duomenų saugumo pažeidimas.

36. Patikimumo vertinimo modeliai yra labai svarbūs siekiant užkirsti kelią duomenų saugumo pažeidimams amžiaus užtikrinimo aplinkybėmis, nes šiais modeliais apibrėžiama, kaip skirtingos šalys gali patikrinti viena kitos tapatybę ir sąžiningumą. Minėti modeliai palengvina saugų ryšio palaikymą ir keitimąsi duomenimis tarp dalyvių, kurie gali neturėti ankstesnių santykių. Be to, pseudonimų suteikimas asmens duomenims ir jų šifravimas gali būti naudingos priemonės siekiant sušvelninti galimą neigiamą duomenų saugumo pažeidimų poveikį. Taip pat labai svarbu gali būti laikytis saugojimo trukmės apribojimo principo ir taikyti trumpus saugojimo laikotarpius, kad amžiaus užtikrinimas būtų saugus, nes minėtais sprendimais sumažinamas vadinamasis poveikio plotas. Vertinga apsaugos priemone gali būti laikoma duomenų neregistravimo politika: patikrinus naudotojo amžių, jokie asmens duomenys, naudoti amžiaus užtikrinimo procesui, neregistruojami.

37. Praktiškai, atsižvelgiant į didėjantį teisinį spaudimą įgyvendinti amžiaus užtikrinimą ir į paslaugų teikėjų, kuriems gali būti taikomos tokios taisyklės, skaičių, reikėtų tikėtis saugumo pažeidimų. Reikėtų įvertinti, ar įgyvendintos visos tinkamos technologinės apsaugos ir organizacinės priemonės, kad nedelsiant būtų nustatyta, ar buvo padarytas pažeidimas, ir, atsižvelgiant į tai, ar atsiranda pareiga pranešti[35]. Vienas iš pagrindinių bet kokios duomenų saugumo politikos elementų yra galimybė, kai įmanoma, užkirsti kelią pažeidimui ir, jei jis padaromas, laiku reaguoti. Todėl gebėjimas greitai atkurti amžiaus užtikrinimo prieinamumą po saugumo pažeidimo taip pat turėtų būti laikomas esminiu. Taip pat labai svarbu pasiekti

[31] Nesusiejimo savybė reiškia, kad neįmanoma susieti arba sugretinti skirtingų duomenų vienetų, veiksmų ar operacijų su konkrečiu duomenų subjektu.

[32] Pasirinktinis atskleidimas yra prieigos raktų, kredencialų ir liudijimų savybė, leidžianti duomenų subjektams kiekvienu konkrečiu atveju su konkrečiomis šalimis dalytis tik duomenų subjekto pageidaujama informacija.

[33] Išdavimas partijomis grindžiamas atsakymu į vieną duomenų subjekto pateiktą kredencialų užklausą, pateikiant tuo pačiu metu parengtą kredencialų rinkinį arba grupę.

[34] Nulinio žinojimo protokolas yra protokolas, pagal kurį viena šalis (patvirtintojas) gali įrodyti kitai šaliai (tikrintojui), kad tam tikras pareiškimas yra teisingas, tikrintojui neperduodant jokios informacijos, išskyrus to pareiškimo teisingumo faktą.

[35] Iš EDAV gairių Nr. 9/2022 dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal BDAR, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_lt.pdf.

amžiaus užtikrinimo ekosistemos atsparumą, pirmenybę teikiant siekiui turėti įvairių alternatyvų ir laisvai susietų šalių[36], kurios nėra tiek priklausomos viena nuo kitos, kad vienos iš jų patiriami trikdžiai arba gedimas sukeltų didelių prieigos apribojimų.

38. Nors vykdant amžiaus užtikrinimą saugumo priemonės yra itin svarbios, jomis negarantuojama, kad leistina ar neleistina prieiga prie asmens duomenų nedarys poveikio fizinių asmenų teisėms. Saugumo priemonės negali pakeisti būtinumo, proporcingumo ar pritaikytosios ir standartizuotosios duomenų apsaugos principų.

2.10 Atskaitomybė

Paslaugų teikėjai ir visos susijusios trečiosios šalys turėtų įgyvendinti valdymo metodus, pagal kuriuos jie galėtų būti atskaitingi už savo požiūrį į amžiaus užtikrinimą ir įrodyti, kad laikosi Duomenų apsaugos reglamento ir kitų teisinių reikalavimų.

39. Atsižvelgiant į tai, kad amžiaus užtikrinimo procese dalyvauja įvairūs suinteresuotieji subjektai, amžiaus užtikrinimo valdymui tenka labai svarbus vaidmuo, kad amžiaus užtikrinamas būtų vykdomas atskaitingai. Amžiaus užtikrinimas turėtų būti vykdomas pagal valdymo sistemą, pasirūpinant, kad visi procesai ir sistemos būtų kuriami, įgyvendinami, peržiūrimi, dokumentuojami, vertinami, naudojami, prižiūrimi, testuojami ar audituojami taip, kad tai atitiktų duomenų apsaugos taisykles ir kitus teisinius reikalavimus. Ši sistema turėtų apimti bent jau duomenų apsaugos politikos priemones (BDAR 24 straipsnio 2 dalis) ir prioritetų nustatymo bei sprendimų priėmimo procesus, kurių reikia, kad būtų pasiekti atitikties tikslai ir per visą amžiaus užtikrinimo ciklą būtų tinkamai valdoma rizika.

40. Pavyzdžiui, valdymo sistemoje turėtų būti apibrėžta, kas ir kaip, žvelgiant iš duomenų valdytojo ir (arba) duomenų tvarkytojo perspektyvos, yra atsakingas už konkrečią su duomenų tvarkymu susijusią veiklą ar operacijas. Taikant minėtą valdymo sistemą, taip pat turėtų būti užtikrinama, kad valdžios institucijos ir atitinkami suinteresuotieji subjektai galėtų veiksmingai audituoti amžiaus užtikrinimą. Valdymo sistema yra labai svarbi ne tik atskaitomybei, bet ir skaidrumui bei pasitikėjimui amžiaus užtikrinimu. Duomenų subjektai labiau linkę pasitikėti metodais, apie kurių veikimą, sprendimų priėmimą ir kt. pateikiama skaidri informacija.

41. Be to, dalis valdymo sistemos apima amžiaus užtikrinimo veiksmingumo įtvirtinimą (2.5 skirsnis), pritaikytąją ir standartizuotąją duomenų apsaugą (2.8 skirsnis) ir saugumą (2.9 skirsnis).

Europos duomenų apsaugos valdybos vardu

[36] Šalys viena nuo kitos priklauso kuo mažiau, todėl, įvykus pokyčiams ar gedimams, sumažėja poveikio mastas.

Pirmininkė

(Anu Talus)

Priimta