Nuomonė 11/2024 dėl veido atpažinimo technologijų naudojimo siekiant racionalizuoti keleivių srautus oro uostuose (suderinamumas su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais)

1.1 redakcija

Priimta 2024 m. gegužės 23 d.

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

Priimta

1.1 redakcija	2024 m. gegužės 28 d.	Gramatinių klaidų nuomonės santraukoje (p. 3 ir 4) ir 77 bei 90 punktuose ištaisymas
1.0 redakcija	2024 m. gegužės 23 d.	Nuomonės priėmimas

Santrauka

Prancūzijos priežiūros institucija paprašė Europos duomenų apsaugos valdybos pateikti nuomonę dėl oro uostų operatorių ir oro transporto bendrovių veido atpažinimo technologijų naudojimo vykdant biometrinį keleivių tapatybės patvirtinimą ar nustatymą, siekiant racionalizuoti keleivių srautus oro uostuose.

Pirmiausia Valdyba primena, kad, naudojant biometrinius duomenis, ypač veido atpažinimo technologijas, kyla didesni pavojai duomenų subjektų teisėms ir laisvėms. Tai susiję su biometrinių duomenų, kuriems pagal BDAR 9 straipsnį taikoma speciali apsauga, tvarkymu. Prieš naudodami šias technologijas, net jei jos būtų laikomos itin veiksmingomis, duomenų valdytojai turėtų įvertinti poveikį duomenų subjektų pagrindinėms teisėms bei laisvėms ir apsvarstyti, ar teisėto šio duomenų tvarkymo tikslo nebūtų galima pasiekti mažiau varžančiomis priemonėmis.

Remiantis prašymu, šios nuomonės taikymo sritis apribota duomenų tvarkymo suderinamumu su **BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais, siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose**, būtent keturiuose kontrolės punktuose, t. y. saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose. Šioje nuomonėje nėra visapusiškai ir išsamiai analizuojama, ar susijęs (-ę) duomenų valdytojas (-ai) ir, jei taikoma, jo (jų) duomenų tvarkytojas (-ai) laikosi kiekvienu atveju Bendrojo duomenų apsaugos reglamento. Todėl ši nuomonė nedaro poveikio teisinei ir techninei kiekvieno konkretaus atvejo analizei remiantis konkrečiu duomenų valdytojo numatytu duomenų tvarkymu ir aplinkybėmis. Be to, taikomo teisinio pagrindo analizė nepatenka į prašyme Valdybai pateiktų klausimų taikymo sritį, todėl sutikimo su šiuo duomenų tvarkymu galiojimas pagal BDAR 6, 7 ir 9 straipsnius šioje nuomonėje nenagrinėjamas. Be to, ši nuomonė nedaro poveikio valstybių narių teisės aktuose nustatytiems biometrinių duomenų apribojimams.

Šioje nuomonėje Valdyba duomenų tvarkymo derėjimą su pirmiau nurodytomis BDAR nuostatomis vertina pagal **keturis konkrečius scenarijus**.

Pagal **pirmąjį scenarijų** užregistruoti biometriniai šablonai saugomi pas asmenis, pvz., individualiuose jų prietaisuose, tik jų žinioje, kad būtų galima patvirtinti keleivių tapatybę (atlikti palyginimą „1 su 1“), jiems einant per pirmiau nurodytus oro uostų kontrolės punktus.

Valdyba daro išvadą, kad pasirinktos priemonės galėtų būti laikomos atitinkančiomis būtinumo principą, jei duomenų valdytojas gali įrodyti, kad nėra alternatyvių mažiau varžančių sprendimų, kuriais tą patį tikslą būtų galima pasiekti taip pat veiksmingai. Be to, varžomąjį duomenų tvarkymo poveikį galima sumažinti aktyviu keleivių dalyvavimu, nes biometriniai šablonai saugomi tik pas juos, pvz., individualiuose jų prietaisuose, tik jų žinioje, o užbaigus atitikties nustatymą jų duomenys netrukus ištrinami. Tuo remdamasi Valdyba daro išvadą, kad pagal pirmąjį scenarijų numatytas duomenų tvarkymas **iš esmės galėtų būti laikomas suderinamu su BDAR 5 straipsnio 1 dalies f punktu ir 25 bei 32 straipsniais**, jei būtų įgyvendintos tinkamos apsaugos priemonės.

Valdyba nustatė apsaugos priemones, kurios būtinai turėtų būti įgyvendinamos pasirinkus į pirmąjį scenarijų panašų sprendimą.

Pagal **antrąjį scenarijų** užregistruoti biometriniai šablonai šifruota forma centralizuotai saugomi oro uoste, o raktus ir (arba) slaptažodžius turi tik keleiviai. Taip, keleiviams einant per pirmiau nurodytus oro uostų kontrolės punktus, galima patvirtinti jų tapatybę (palyginimas „1 su 1“). Registracija galioja

tam tikrą laikotarpį, kuris, pvz., galėtų siekti nuo vienų metų po paskutinio skrydžio iki paso galiojimo pabaigos datos.

Valdyba daro išvadą, kad šis duomenų tvarkymas galėtų būti laikomas atitinkančiu būtinumo principą, jei duomenų valdytojas gali įrodyti, kad nėra alternatyvių mažiau varžančių sprendimų, kuriais tą patį tikslą būtų galima pasiekti taip pat veiksmingai. Be to, varžomąjį duomenų tvarkymo poveikį galima sumažinti aktyviu keleivių dalyvavimu, nes jie turi vien jų žinioje esančius užšifruotiems jų biometriniams duomenims skirtus raktus ir (arba) slaptažodžius. Darant prielaidą, kad duomenų valdytojas įgyvendina tinkamas apsaugos priemones, pagal šį scenarijų naudojant centralizuotą duomenų bazę kylantys pavojai saugumui galėtų būti sumažinami, o neigiamas poveikis duomenų subjektų pagrindinėms teisėms ir laisvėms galėtų būti laikomas proporcingu numatomai naudai. Saugojimo trukmės apribojimo principo atžvilgiu pažymėtina, kad Valdybai nepateikta informacijos, kuria būtų pagrįstas ilgas saugojimo laikotarpis. Siekdami pagal šį scenarijų užtikrinti derėjimą su BDAR 5 straipsnio 1 dalies e punktu, duomenų valdytojai turėtų turėti galimybę pagrįsti, kodėl konkrečiais atvejais reikia numatyto saugojimo laikotarpio. Valdyba rekomenduoja, kad duomenų valdytojai numatytų kuo trumpesnį saugojimo laikotarpį ir pasiūlytų keleiviams galimybę nusistatyti pageidaujamą saugojimo laikotarpį. Tuo remdamasi Valdyba daro išvadą, kad pagal 2 scenarijų numatytas duomenų tvarkymas **iš esmės galėtų būti laikomas suderinamu su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais**, jei būtų įgyvendintos tinkamos apsaugos priemonės.

Valdyba nustatė apsaugos priemones, kurios būtinai turėtų būti įgyvendinamos pasirinkus į antrąjį scenarijų panašų sprendimą.

Pagal **trečiąją scenarijų** užregistruoti biometriniai šablonai šifruota forma centralizuotai saugomi oro uoste oro uosto operatoriaus žinioje. Taip, keleiviams einant per pirmiau nurodytus oro uosto kontrolės punktus, galima nustatyti jų tapatybę (palyginimas „1 su N“). Pagal šį scenarijų saugojimo laikotarpis paprastai yra 48 valandos, o duomenys ištrinami, kai tik lėktuvas pakyla.

Kadangi tapatybės ir biometriniai duomenys saugomi centrinėje duomenų bazėje, vėliau, jei būtų pažeistas duomenų bazės saugumas, gali būti įgyjama prieiga prie viso duomenų rinkinio ir atsirasti galimybė neleistinai arba neteisėtai nustatyti keleivių tapatybę kitose aplinkose. Oro uosto operatoriaus žinioje esančioje centralizuoto saugojimo struktūroje keleiviai taip pat labiau praranda savo duomenų kontrolę. Valdyba mano, kad panašų keleivių srautų racionalizavimo oro uostuose rezultatą galima pasiekti mažesnio poveikio suvaržymu, o neigiamas poveikis duomenų subjektų pagrindinėms teisėms ir laisvėms, kuris atsirastų dėl duomenų pažeidimo centralizuotoje biometrinių duomenų bazėje, atrodo, nusveria numatomą šio duomenų tvarkymo naudą. Todėl šis duomenų tvarkymas negali atitikti būtinumo ir proporcingumo principų. Tuo remdamasi Valdyba daro išvadą, kad pagal trečiąjį scenarijų numatytas duomenų tvarkymas **negali būti suderinamas su BDAR 25 straipsniu**. Be to, jei duomenų valdytojai apsiribotų tik pagal šį scenarijų aprašytomis priemonėmis, šis duomenų tvarkymas **neatitiktų BDAR 5 straipsnio 1 dalies f punkto ir 32 straipsnio**.

Pagal **ketvirtąjį scenarijų** užregistruoti biometriniai šablonai šifruota forma centralizuotai saugomi debesijoje oro transporto bendrovės arba jos debesijos paslaugų teikėjo žinioje. Taip, keleiviams einant per pirmiau nurodytus oro uosto kontrolės punktus, galima nustatyti jų tapatybę (palyginimas „1 su N“). Saugojimo laikotarpis pagal šį scenarijų galėtų trukti tol, kol klientas turi paskyrą toje oro transporto bendrovėje.

Kadangi tapatybės ir biometriniai duomenys saugomi centrinėje duomenų bazėje debesijoje, prieigą prie šių duomenų galėtų turėti keli subjektai, taip pat galbūt ne EEE paslaugų teikėjai. Naudojimo metu keleivių duomenys iššifruojami, o raktai yra oro transporto bendrovės arba jos duomenų tvarkytojų

žinioje, todėl galėtų padidėti pavojų saugumui perimetras. Taikant tokią centralizuoto saugojimo struktūrą, keleiviai taip pat labiau praranda savo duomenų kontrolę. Be to, duomenys galėtų būti saugomi labai ilgą laikotarpį, todėl jiems kyla didesnis saugumo pažeidimų pavojus ir, atrodo, viršijama tai, kas tikrai būtina ir proporcinga duomenų tvarkymo tikslais, nebent imamasi daugiau akivaizdžių priemonių asmenims kylantiems pavojams sumažinti.

Valdyba mano, kad panašų keleivių srautų racionalizavimo oro uostuose rezultatą galima pasiekti mažesnio poveikio suvaržymu, o neigiamas poveikis duomenų subjektų pagrindinėms teisėms ir laisvėms, kuris galėtų atsirasti dėl duomenų pažeidimo centralizuotoje biometrinių duomenų bazėje, atrodo, nusveria numatomą šio duomenų tvarkymo naudą. Todėl šis duomenų tvarkymas negali atitikti būtinumo ir proporcingumo principų. Tuo remdamasi Valdyba daro išvadą, kad pagal ketvirtąjį scenarijų numatytas duomenų tvarkymas **negali būti suderinamas su BDAR 25 straipsniu**. Be to, remiantis Valdybos turima informacija, šis duomenų tvarkymas **neatitiktų BDAR 5 straipsnio 1 dalies e punkto**, o jei duomenų valdytojai apsiribotų tik pagal šį scenarijų aprašytomis priemonėmis, **jis neatitiktų BDAR 5 straipsnio 1 dalies f punkto ir 32 straipsnio**.

Turinys

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento 2016/679/ES dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – **BDAR**) 63 straipsnį ir 64 straipsnio 2 dalį,

atsižvelgdama į EEE susitarimą, ypač į jo XI priedą ir 37 protokolą, su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į Europos duomenų apsaugos valdybos (toliau – **Valdyba** arba **EDAV**) darbo tvarkos taisyklių (toliau – **EDAV DTT**) 10 ir 22 straipsnius,

kadangi:

(1) pagrindinė Valdybos užduotis yra užtikrinti nuoseklų BDAR taikymą visoje Europos ekonominėje erdvėje (toliau – **EEE**). BDAR 64 straipsnio 2 dalyje nurodyta, kad bet kuri priežiūros institucija (toliau – **PI**), valdybos pirmininkas arba Europos Komisija gali prašyti, kad Valdyba išnagrinėtų bet kurį bendro pobūdžio klausimą arba klausimą, kuris daro poveikį daugiau nei vienoje EEE valstybėje narėje, ir pateiktų nuomonę;

(2) pagal BDAR 64 straipsnio 3 dalį kartu su EDAV DTT 10 straipsnio 2 dalimi Valdyba priima nuomonę per aštuonias savaites po to, kai pirmininkas ir kompetentinga PI nusprendžia, kad pateikti dokumentai yra išsamūs. Atsižvelgiant į klausimo sudėtingumą, pirmininko sprendimu šis laikotarpis gali būti pratęstas dar šešioms savaitėms,

priėmė šią nuomonę:

1 ĮVADAS

1.1 Faktų santrauka

1. 2024 m. vasario 16 d. Prancūzijos priežiūros institucija (toliau – **Prancūzijos PI**) paprašė Valdybos pateikti nuomonę dėl oro uostų operatorių ir oro transporto bendrovių veido atpažinimo technologijų naudojimo biometriniam keleivių[2] tapatybės patvirtinimui ar nustatymui, siekiant racionalizuoti keleivių srautus oro uostų saugumo kontrolės punktuose[3], bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose (išskyrus sienų kontrolę ir neapmuitinamų parduotuvių atliekamus patikrinimus), suderinamumo su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais (toliau – **Prašymas**). Prie Prašymo Prancūzijos PI pridėjo tipinių naudojimo atvejų aprašą (I priedas).

[1] Šioje nuomonėje daromos nuorodos į **valstybes nares** turėtų būti suprantamos kaip nuorodos į EEE valstybes nares. Šioje nuomonėje daromos nuorodos į Sąjungą arba ES turėtų būti suprantamos kaip nuorodos į EEE.
[2] Šioje nuomonėje **keleiviu** vadinamas duomenų subjektas, kurio asmens duomenys tvarkomi konkrečiu šioje nuomonėje aprašytu tikslu. Toliau šioje nuomonėje sąvokos keleivis ir asmuo vartojamos ta pačia reikšme.
[3] Šioje nuomonėje nurodytuose **oro uostų saugumo kontrolės punktuose** oro uosto operatoriaus atsakomybe atliekami saugumo patikrinimai, kuriuose keleiviai turi dalyvauti, kad iš išvykimo salės galėtų patekti į įlaipinimo zoną arba prie įlaipinimo vartų.

2. Prašyme Prancūzijos PI nurodo, kad šiuo metu keliuose ES oro uostuose išbandomi modeliai skirtingose valstybėse narėse skiriasi, todėl gali kilti skirtingo priežiūros institucijų aiškinimo ir skirtingo poveikio ES duomenų subjektų pagrindinėms teisėms ir laisvėms pavojų[4].

3. Valdyba mano, kad, norint pateikti atsakymą į Prašymą, reikia atsakyti į toliau išvardytus klausimus.

4. **1 klausimas**

1.1. Ar veido atpažinimo technologijos naudojimas biometriniam tapatybės patvirtinimui, siekiant **konkrečiai racionalizuoti keleivių srautus oro uostuose** (saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose), gali būti suderinamas su **BDAR 5 straipsnio 1 dalies f punktu ir 25 bei 32 straipsniais**, kai naudojama saugojimo struktūra, kurią naudojant kiekvieno keleivio biometrinį šabloną saugo **tik asmuo**, pvz., tik jo kontroliuojamame asmeniniame prietaise?

1.2. Jei šis duomenų tvarkymas būtų laikomas suderinamu su pirmiau nurodytomis nuostatomis, kokių būtiniausių tinkamų apsaugos priemonių reikėtų imtis atsižvelgiant į BDAR 25 ir 32 straipsnius?

2 klausimas

2.1. Ar veido atpažinimo technologijos naudojimas biometriniam tapatybės patvirtinimui ar nustatymui, siekiant **konkrečiai racionalizuoti keleivių srautus oro uostuose** (saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose), gali būti suderinamas su **BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais**, kai taikoma **centralizuoto** saugojimo struktūra, kurią naudojant kiekvieno keleivio biometrinis šablonas saugomas centrinėje duomenų bazėje:

2.1.1. centrinėje duomenų bazėje oro uoste oro uosto operatoriaus žinioje šifruota forma, kad būtų galima patvirtinti tapatybę, kai raktą ir (arba) slaptažodį turi tik asmuo (pvz., savo mobiliajame telefone)?

2.1.2. Jei šis duomenų tvarkymas būtų laikomas suderinamu, kokių būtiniausių tinkamų apsaugos priemonių reikėtų imtis atsižvelgiant į BDAR 25 ir 32 straipsnius?

2.2.1. Centrinėje duomenų bazėje oro uoste oro uosto operatoriaus žinioje šifruota forma tapatybei nustatyti, kai raktus turi oro uosto operatorius?

2.2.2. Jei šis duomenų tvarkymas būtų laikomas suderinamu, kokių būtiniausių tinkamų apsaugos priemonių reikėtų imtis atsižvelgiant į BDAR 25 ir 32 straipsnius?

2.3.1. Debesijoje oro transporto bendrovės arba jos paslaugų teikėjo (duomenų tvarkytojo) žinioje šifruota forma tapatybei nustatyti, kai raktus turi oro transporto bendrovė arba jos paslaugų teikėjas?

2.3.2. Jei šis duomenų tvarkymas būtų laikomas suderinamu, kokių būtiniausių tinkamų apsaugos priemonių reikėtų imtis atsižvelgiant į BDAR 25 ir 32 straipsnius?

[4] Prašymas, p. 1.

5. Prancūzijos priežiūros institucijai 2024 m. vasario 16 d., o Valdybai – 2024 m. vasario 23 d. nusprendus, kad duomenų rinkinys yra išsamus, sekretoriatas 2024 m. vasario 23 d. jį išplatino. EDAV pirmininkė nusprendė, kad, laikantis BDAR 64 straipsnio 3 dalies kartu su EDAV DTT 10 straipsnio 2 dalimi, standartinis aštuonių savaičių laikotarpis dėl dalyko sudėtingumo pratęsiamas dar šešioms savaitėms.

1.2 Prašymo pateikti nuomonę pagal BDAR 64 straipsnio 2 dalį priimtinumas

6. BDAR 64 straipsnio 2 dalyje nustatyta, kad visų pirma bet kuri PI gali prašyti, kad Valdyba išnagrinėtų bet kurį bendro pobūdžio klausimą arba klausimą, kuris daro poveikį daugiau nei vienoje valstybėje narėje, ir kad ji pateiktų nuomonę.

7. Valdyba mano, kad Prancūzijos PI pateiktas Prašymas dėl veido atpažinimo technologijos naudojimo biometriniam tapatybės patvirtinimui ar nustatymui, siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose, suderinamumo yra susijęs su klausimais „kurie daro poveikį daugiau nei vienoje valstybėje narėje“, nes, kaip paaiškinta Prašyme[5], šiuo metu valstybių narių oro uostuose įgyvendinami keli projektai ir prognozuojama, kad artimiausiais metais šis naudojimas didės. Šiuo metu įvairiuose oro uostuose ir įvairių oro transporto bendrovių išbandomi modeliai skirtingose valstybėse narėse labai skiriasi, todėl gali atsirasti pavojus, kad duomenų apsaugos požiūriu gali atsirasti skirtingas poveikis daugiau nei vienoje valstybėje narėje.

8. Be to, Valdyba mano, kad Prancūzijos PI pateiktas Prašymas yra svarbus BDAR 5 straipsnio 1 dalies e ir f punktuose nustatytų principų, BDAR 25 straipsnyje nustatytų duomenų valdytojams taikomų reikalavimų ir BDAR 32 straipsnyje nustatytų duomenų valdytojams ir tvarkytojams taikomų reikalavimų taikymo atžvilgiu. Todėl šis Prašymas pateiktas BDAR 64 straipsnio 2 dalyje nurodytu „bendro pobūdžio klausimu“, nes yra susijęs su nuosekliu saugojimo trukmės apribojimo (BDAR 5 straipsnio 1 dalies e punktas), vientisumo ir konfidencialumo (BDAR 5 straipsnio 1 dalies f punktas) principų, pritaikytosios ir standartizuotosios duomenų apsaugos (BDAR 25 straipsnis) ir duomenų saugumo (BDAR 32 straipsnis) sąvokų aiškinimu, siekiant, be kita ko, užtikrinti nuoseklų šių nuostatų taikymą EEE.

9. Bet kokie galimi valstybių narių pozicijų dėl BDAR 5 straipsnio 1 dalies e bei f punktų ir 25 bei 32 straipsnių aiškinimo skirtumai padidintų pavojų, kad oro uostų operatorių ir oro transporto bendrovių vykdomi veido atpažinimo projektai bus plėtojami nenuosekliai. Kadangi Prancūzijos PI įrodė akivaizdžią nuoseklaus šių nuostatų aiškinimo būtinybę dėl veido atpažinimo technologijos naudojimo biometriniam keleivių tapatybės patvirtinimui ir nustatymui, siekiant racionalizuoti keleivių srautus oro uostuose, atžvilgiu[6], remdamasi EDAV DTT 10 straipsnio 3 dalimi Valdyba mano, kad prašymas yra pagrįstas.

10. Pagal BDAR 64 straipsnio 3 dalį EDAV nuomonės neteikia, jei jau yra pateikusi nuomonę tuo klausimu[7]. Atsakymų į Prašyme pateiktus klausimus EDAV pateikusi dar nėra. Nors EDAV gairėse 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus[8] jau nurodyti keli naudingi su tvarkant

[5] Prašymas, p. 3.
[6] Prašymas, p. 1–3.
[7] BDAR 64 straipsnio 3 dalis ir EDAV darbo tvarkos taisyklių 10 straipsnio 4 dalis.
[8] 2020 m. sausio 29 d. priimtų EDAV gairių 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus 2.0 redakcija (toliau – **EDAV gairės 3/2019 dėl vaizdo prietaisų**).

biometrinių duomenų tvarkymui taikytinomis saugumo priemonėmis susiję dalykai, jose neišnagrinėti visi su Prašyme pateiktais klausimais susiję aspektai. Be to, esamose EDAV gairėse, įskaitant Gaires 3/2019 dėl vaizdo prietaisų, nepateikta konkrečių gairių dėl galimų aspektų, kuriuos reikėtų patikrinti dėl centralizuoto arba decentralizuoto biometrinių duomenų saugojimo keleivių tapatybei nustatyti arba patvirtinti, siekiant racionalizuoti keleivių srautus oro uostuose, ir šio duomenų tvarkymo suderinamumo su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais.

11. Dėl šių priežasčių Valdyba mano, kad Prašymas yra priimtinas, o jame pateiktus klausimus reikėtų išnagrinėti pagal BDAR 64 straipsnio 2 dalį priimamoje nuomonėje.

2 NUOMONĖS TAIKYMO SRITIS IR APLINKYBĖS

2.1 Nuomonės taikymo sritis

12. Šioje nuomonėje, remiantis Prašymu, nagrinėjamas tik oro uostų operatorių ir oro transporto bendrovių veido atpažinimo technologijos naudojimo biometriniam keleivių tapatybės patvirtinimui ar nustatymui **siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose**, būtent – saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose, suderinamumas su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais.

13. **Dėl šios nuomonės taikymo srities** Valdyba paaiškina kad:

    1) į šios nuomonės taikymo sritį nepatenka asmens duomenų tvarkymas vykdant sienų kontrolę arba patikrinimus neapmuitinamose parduotuvėse, nes juos vykdo ne oro uostų operatoriai ir oro transporto bendrovės, bet kiti duomenų valdytojai;

    2) į šios nuomonės taikymo sritį nepatenka veido atpažinimo technologijos naudojimas bet kokiais kitais (pvz., teisėsaugos) tikslais, net jei jis grindžiamas toliau 3.2 skirsnyje aprašytais scenarijais, arba bet kokių kitų šalių veido atpažinimo technologijų naudojimas, net jei tai būtų panašūs tikslai;

    3) šioje nuomonėje nagrinėjamas tik keleivių asmens duomenų tvarkymas, o kitų tipų duomenų subjektai, pvz., oro uostų operatorių arba oro transporto bendrovių darbuotojai, į jos taikymo sritį nepatenka;

    4) šioje nuomonėje nagrinėjamas Prancūzijos PI pateiktas Prašymas, susijęs su keleivių biometrinių šablonų saugojimo struktūrų suderinamumu su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais. Šiuo atžvilgiu šioje nuomonėje nėra visapusiškai ir išsamiai analizuojama, kaip susijęs (-ę) duomenų valdytojas (-ai) ir, jei taikoma, jo (jų) duomenų tvarkytojas (-ai) kiekvienu atveju laikosi BDAR. Tai itin svarbu atsižvelgiant į tai, kad šios technologijos kelia didesnius su specialių kategorijų duomenų tvarkymu pagal BDAR 9 straipsnį susijusius pavojus. Todėl ši nuomonė nedaro poveikio su kitomis BDAR nuostatomis susijusiam vertinimui dėl veido atpažinimo technologijų naudojimo, taip pat Prašyme nurodytame konkrečiame sektoriuje, arba teisinei ir techninei konkrečių atvejų analizei, grindžiamai konkrečiu duomenų valdytojo numatytu duomenų tvarkymu ir aplinkybėmis;

    5) šioje nuomonėje nenagrinėjamas vaikų asmens duomenų tvarkymas, todėl ji nedaro poveikio jokiems konkretiems šiuo atžvilgiu taikomiems reikalavimams;

6) ši nuomonė nedaro poveikio valstybių narių nacionalinės teisės aktuose nustatytiems teisiniams biometrinių duomenų naudojimo reikalavimams ir kitiems susijusiems apribojimams[9];

7) jokia šioje nuomonėje padaryta išvada nedaro poveikio tolesniems technologiniams pokyčiams;

8) šioje nuomonėje nagrinėjami keturi scenarijai, kurių konkretūs požymiai aprašyti toliau 3.2 skirsnyje. Joje nenagrinėjami kitokie scenarijai, net jei duomenys tvarkomi tais pačiais tikslais.

14. Prašyme Prancūzijos PI nurodė, kad keleivių biometrinių duomenų tvarkymas siekiant racionalizuoti keleivių srautus oro uostuose būtų grindžiamas prielaida, kad asmenys su šiuo duomenų tvarkymu sutinka, ir tai galbūt sudarytų teisinį pagrindą pagal BDAR[10]. **Vis dėlto taikomo teisinio pagrindo analizė nepatenka į Prašyme Europos duomenų apsaugos valdybai pateiktų klausimų taikymo sritį, todėl sutikimo su šiuo duomenų tvarkymu galiojimas pagal BDAR 6, 7 ir 9 straipsnius šioje nuomonėje nenagrinėjamas.**

15. Vis dėlto EDAV apskritai atkreipia dėmesį į tai, kad, norėdami remtis šiuo teisiniu pagrindu, susiję duomenų valdytojai turėtų gauti aiškų galiojantį sutikimą iš naudotis šiomis paslaugomis pageidaujančių asmenų[11]. Šis aiškus sutikimas turėtų būti duotas laisva valia, būti konkretus ir pagrįstas[12], o tai, ar šios sąlygos įvykdytos, būtų analizuojama kiekvienu konkrečiu atveju. Be kita ko, tai reiškia, kad:

1) asmenys turėtų turėti galimybę bet kada ir be pasekmių lengvai atšaukti šį sutikimą[13];

2) kad sutikimas būtų duotas laisva valia, šios biometrinės technologijos gali būti naudojamos tik savanoriškai, nes asmenys turi turėti galimybę laisva valia pasirinkti, ar naudotis šiomis paslaugomis be pasekmių (tokių kaip daug ilgesnis laukimas, jeigu keleiviai neduoda sutikimo[14]), paskatų, papildomų išlaidų arba papildomų lengvatų kaip atlygio[15];

3) aiškaus sutikimo taip pat reikėtų prašyti iš asmenų, kurių biometriniai duomenys tvarkomi, net jei jie nėra užsiregistravę tam, kad jų tapatybė būtų nustatoma arba

[9] Pavyzdžiui, BDAR 9 straipsnio 4 dalyje nurodyta, kad valstybės narės gali toliau taikyti arba nustatyti papildomas su biometrinių duomenų tvarkymu susijusias sąlygas, įskaitant apribojimus.
[10] Prašymas, I priedas.
[11] Pagal BDAR 4 straipsnio 14 punktą, 9 straipsnio 1 dalį ir 9 straipsnio 2 dalies a punktą biometrinių duomenų tvarkymas vien fizinio asmens tapatybės nustatymo tikslu draudžiamas, nebent duomenų subjektas yra davęs aiškų sutikimą tvarkyti šiuos asmens duomenis vienu arba keliais konkrečiais tikslais, išskyrus atvejus, kai pagal Sąjungos arba valstybės narės teisę nustatyta, kad BDAR 9 straipsnio 1 dalyje nustatyto draudimo duomenų subjektas panaikinti negali. Taip pat žr. BDAR 51, 52 ir 53 konstatuojamąsias dalis.
[12] BDAR 4 straipsnio 11 punktas ir 7 straipsnis.
[13] BDAR 7 straipsnio 4 dalis, taip pat žr. BDAR 50 konstatuojamąją dalį.
[14] Pavyzdžiui, tai gali apimti pasvarstymus, pvz., dėl sistemos sukūrimo, siekiant išvengti socialinio spaudimo sutikti nenorintiems keleiviams ir taip vengiant, kad toks pasirinkimas turėtų neigiamo poveikio kitiems keleiviams.
[15] 2020 m. gegužės 4 d. priimtų 1.1 redakcijos EDAV gairių 05/2020 dėl sutikimo pagal Reglamentą 2016/679 (toliau – **EDAV gairės 5/2020 dėl sutikimo**) 46 ir 48 punktai.

patvirtinama šiomis priemonėmis. Kitaip tariant, labai svarbu, kad kameromis nebūtų skenuojami asmenų, kurie nėra davę aiškaus sutikimo dėl veido atpažinimo numatytu tikslu, veidai. Tai užtikrinti galima, pvz., veido atpažinimui skiriant specialius takus, juos tinkamai paženklinant ir fiziškai atskiriant nuo nebiometrinės kontrolės srautų, kad šiuos takus būtų galima aiškiai atpažinti;

4) nedarant poveikio tam, ar šiam duomenų tvarkymui sutikimas būtų taikytinas teisinis pagrindas, BDAR 5 straipsnyje nustatyti su duomenų tvarkymo būtinumu ir proporcingumu susiję duomenų tvarkymo principai vis tiek taikomi, net jei asmenys yra davę aiškų sutikimą naudoti jų biometrinius duomenis[16].

16. Prašyme nurodyta[17], kad tvarkydami duomenis oro uostų saugumo kontrolės punktuose oro uostų operatoriai veiktų kaip duomenų valdytojai, o oro transporto bendrovės veiktų kaip duomenų valdytojos duomenų tvarkymo bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamųjų vietose. Todėl Valdyba atkreipia dėmesį į tai, kad Prašyme aprašyto duomenų tvarkymo veikloje gali dalyvauti įvairūs dalyviai ir kad ji nevertino (bendro) duomenų valdytojo ir duomenų tvarkytojo vaidmenų taikymo pagal toliau šios nuomonės 3.2 skirsnyje aprašytus scenarijus. Kad būtų įvykdyti BDAR reikalavimai, kiekvienu atveju reikės nustatyti susijusius dalyvius ir aiškiai priskirti jiems funkcijas[18].

17. Be to, Valdyba pažymi, kad šiuo metu Europos Sąjungoje netaikomas vienodas teisinis reikalavimas, kad oro uostų operatoriai ir oro transporto bendrovės visuose pirmiau nurodytuose kontrolės punktuose nustatytų keleivių tapatybę ir tikrintų, kad keleivių įlaipinimo talonuose nurodytas vardas ir pavardė atitiktų jų asmens tapatybės dokumentus[19]. Todėl bet kokiems tokiems reikalavimams taikomi nacionalinės teisės aktai, o jie įvairiose valstybėse narėse gali skirtis. Kai kuriose valstybėse narėse atlikti tokį patikrinimą gali būti reikalaujama kai kuriuose kontrolės punktuose (pvz., bagažo pridavimo arba įlaipinimo vietose), o kitose valstybėse narėse atlikti tokių patikrinimų šiuo metu nereikalaujama[20]. Tai, ar teisinė pareiga tikrinti keleivių tapatybę yra taikoma, tiesiogiai veikia įvairią oro uostų veiklą.

18. Todėl šiose situacijose, **kai nereikalaujama tikrinti keleivių tapatybių pagal oficialius asmens tapatybės dokumentus, biometrinis tikrinimas neturėtų būti atliekamas, nes dėl to atsirastų perteklinis duomenų tvarkymas, kadangi reikėtų tvarkyti daugiau duomenų nei dabartinėje situacijoje, ir taip būtų viršijama tai, kas būtina susijusiam tikslui pasiekti, todėl būtų pažeidžiamas**

[16] Ten pat, 5 punktas.
[17] Prašymas, I priedas.
[18] Pagal BDAR 4 straipsnio 7 ir 8 punktus, 5 straipsnio 2 dalį, 24, 26, 28 ir 29 straipsnius. Taip pat žr. 2021 m. liepos 7 d. priimtų EDAV gairių Nr. 07/2020 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ pagal BDAR 2.1 redakciją.
[19] Susijęs ES lygmens teisės aktas yra 2015 m. lapkričio 5 d. Komisijos įgyvendinimo reglamentas (ES) 2015/1998, kuriuo nustatomos išsamios bendrųjų pagrindinių aviacijos saugumo standartų įgyvendinimo priemonės. Vis dėlto šiame reglamente nesprendžiamas oficialių asmens tapatybės dokumentų patikros oro uostų kontrolės punktuose klausimas – valstybės narės jį gali reguliuoti savo nuožiūra nacionaliniu lygmeniu.
[20] Vadinasi, šiuo metu patikrinimų neatliekama visiškai arba tik tikrinama, ar yra įlaipinimo talonas. Pavyzdžiui, remiantis 1954 m. gegužės 22 d. Protokolu dėl Danijos, Suomijos, Norvegijos ir Švedijos piliečių atleidimo nuo pareigos turėti pasą arba leidimą gyventi gyvenant kitoje Skandinavijos šalyje nei jų gimtoji šalis, nuo 1954 m. liepos 1 d. Norvegijos, Danijos, Suomijos ir Švedijos piliečiai atleidžiami nuo pareigos keliaujant tarp šių šalių turėti pasą arba kitą kelionei skirtą asmens tapatybės dokumentą.

BDAR 5 straipsnio 1 dalies c punkte nustatytas duomenų kiekio mažinimo principas. Į tai reikėtų atkreipti dėmesį nagrinėjant visus toliau šios nuomonės 3.2 skirsnyje aprašytus scenarijus.

2.2 Pagrindinės sąvokos

19. Kad duomenis būtų galima laikyti biometriniais duomenimis pagal BDAR 4 straipsnio 14 punktą[21], neapdorotų duomenų, pvz., duomenys apie fizinio asmens fizines, fiziologines arba elgesio savybes, tvarkymas turėtų apimti šių savybių vertinimą, nes biometriniai duomenys gaunami atlikus šiuos vertinimus[22].

20. Naudojant asmens veido atvaizdą (nuotrauką arba vaizdo įrašą), vadinamą biometrinių duomenų **pavyzdžiu**, galima išgauti skaitmeninį šio veido skiriamųjų bruožų atvaizdą (tai vadinama **šablonu**)[23]. Valdyba taip pat primena, kad „[b]iometrinių duomenų šablonas – tai unikalių savybių, kurios buvo paimtos iš biometrinių duomenų pavyzdžio ir gali būti saugomos biometrinių duomenų bazėje, skaitmeninis atvaizdas“[24], pagal kurį galima konkrečiai nustatyti arba patvirtinti asmens tapatybę. Be to, „[š]is biometrinis šablonas turi būti unikalus ir būdingas konkrečiam asmeniui ir iš esmės laikui bėgant išlieka nuolatinis“[25]. Paprastai atliekant palyginimą, siekiant nustatyti arba patvirtinti asmens tapatybę naudojantis veido atpažinimo technologija, gaunamas biometrinis šablonas lyginamas su saugomais objektais siekiant patikrinti, ar jie vienas kitą atitinką, arba jų ieškoti duomenų bazėje[26].

21. Veido atpažinimo technologija gali atlikti dvi skirtingas funkcijas: tapatybės patvirtinimo[27] ir tapatybės nustatymo[28]. Nors šios dvi funkcijos yra skirtingos, jos abi yra grindžiamos su identifikuotu arba identifikuojamu fiziniu asmeniu susijusių biometrinių duomenų tvarkymu[29], todėl tai yra BDAR 9 straipsnyje nurodytas specialių kategorijų asmens duomenų tvarkymas[30].

---

[21] Taip pat žr. BDAR 51, 52 ir 53 konstatuojamąsias dalis.
[22] EDAV gairių 3/2019 dėl vaizdo prietaisų 74 punktas.
[23] 2023 m. balandžio 26 d. priimtų EDAV gairių 05/2022 dėl veido atpažinimo technologijos naudojimo teisėsaugos srityje 2.0 redakcijos (toliau – **EDAV gairės 5/2022 dėl veido atpažinimo teisėsaugos srityje**) 7 ir 8 punktai.
[24] Ten pat, 9 punktas.
[25] Ten pat.
[26] EDAV gairių 05/2022 dėl veido atpažinimo teisėsaugos srityje 10–11 punktai, taip pat žr. tarptautinį standartą ISO/IEC 2382-37, 2022-03 adresu https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [paskutinį kartą peržiūrėta 2024 m. gegužės 23 d.] (toliau – **ISO/IEC 2382-37**)
[27] Valdyba taip pat atkreipia dėmesį į tai, kad būsimo Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) (jis *Oficialiajame leidinyje* dar nepaskelbtas) 3 straipsnio 36 punkte biometrinis sutikrinimas taip pat apibrėžiamas kaip „automatizuotas vieno su vienu fizinių asmenų tapatybės tikrinimas, įskaitant autentiškumo patvirtinimą, lyginant jų biometrinius duomenis su anksčiau pateiktais biometriniais duomenimis“ (žr. 2024 m. kovo 13 d. Europos Parlamento teisėkūros rezoliuciją dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros aktai (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).
[28] Ten pat, Dirbtinio intelekto akto 3 straipsnio 35 punkte biometrinis tapatybės nustatymas apibrėžiamas kaip „automatinis žmogaus fizinių, fiziologinių, elgesio ar psichologinių požymių atpažinimas siekiant nustatyti fizinio asmens tapatybę, lyginant to asmens biometrinius duomenis su duomenų bazėje saugomais asmenų biometriniais duomenimis“.
[29] ISO/IEC 2382-37.
[30] BDAR 4 straipsnio 14 punktas ir EDAV gairių 05/2022 dėl veido atpažinimo teisėsaugos srityje 12 punktas.

22. Konkrečiai:

tapatybės patvirtinimo tikslas – patvirtinti su biometriniais duomenimis susijusį teiginį, atliekant palyginimą. Jis taip pat vadinamas patikrinimu „1 su 1“;

tapatybės nustatymo tikslas – atlikti paiešką biometrinių duomenų registravimo duomenų bazėje, siekiant pateikti vienam asmeniui priskiriamus identifikatorius. Jis taip pat vadinamas nustatymu „1 su daugeliu“.

23. Abiem (t. y. tapatybės nustatymo ir tapatybės patvirtinimo) atvejais veido atpažinimo metodai grindžiami apskaičiuotąja šablonų atitiktimi, t. y. lyginamo šablono ir bazinio (-ių) lygio (-ių). Šiuo požiūriu jie yra tikimybiniai: lyginant išvedama didesnė ar mažesnė tikimybė, kad asmuo iš tikrųjų yra asmuo, kurio tapatybė turi būti patvirtinta arba nustatyta; jeigu ši tikimybė viršija tam tikrą nustatytą sistemos ribinę vertę, kurią apibrėžia sistemos naudotojas arba kūrėjas, sistema daro prielaidą, kad yra atitiktis, kurią reikia nustatyti arba patvirtinti[31].

[31] EDAV gairių 05/2022 dėl veido atpažinimo teisėsaugos srityje 11 punktas. Taip pat žr. ISO/IEC 2382-37.

3 DĖL PRAŠYMO ESMĖS

3.1 Bendrosios pastabos

24. Šiame skirsnyje analizuojami pirmiau 4 punkte nurodyti klausimai. Šiuo atžvilgiu Valdyba 1-uoju klausimu analizuos suderinamumą su BDAR 5 straipsnio 1 dalies f punktu ir 25 bei 32 straipsniais, o 2-uoju klausimu – suderinamumą su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais.

25. Šiuo tikslu Valdyba analizuos keturis skirtingus scenarijus[32], kurių konkretūs požymiai aprašyti toliau 3.2 skirsnyje.

26. Pirmiausia Valdyba primena, kad, naudojant biometrinius duomenis, ypač veido atpažinimo technologijas, kyla didesni pavojai duomenų subjektų teisėms ir laisvėms. Visų pirma pažymėtina, kad nagrinėjamas duomenų tvarkymas yra susijęs su biometriniais duomenimis, kuriems pagal BDAR 9 straipsnį taikoma speciali apsauga. Ypač pažymėtina, kad biometriniai duomenys negrįžtamai pakeičia santykį tarp kūno ir tapatybės, nes dėl šių duomenų žmogaus kūno savybes galima apdoroti kompiuteriais ir naudoti toliau[33]. Be to, naudojant veido atpažinimo technologiją, gali kilti su klaidingais neigiamais rezultatais, šališkumu ir diskriminacija susijusių pavojų[34], o naudojant biometrinius duomenis netinkamai, pvz., suklastojus tapatybę arba apsimetinėjant, asmenims galėtų būti sukeliama sunkių padarinių[35]. Taip pat pažymėtina, kad, taikant nuotolinį veido atpažinimą be aktyvaus duomenų subjektų dalyvavimo, asmenys apie šį duomenų tvarkymą ir susijusius pavojus gali būti informuoti dar mažiau. Galiausiai svarbu pabrėžti, kad savybės, kuriomis grindžiami biometriniai duomenys, apskritai gali būti laikomos nuolatinėmis ir turėtų būti laikomos neatšaukiamomis, ypač veido atpažinimo atžvilgiu[36].

27. Todėl, atsižvelgiant į tai, kas išdėstyta pirmiau, pažymėtina, kad, prieš naudodami šias technologijas, net jei jos būtų laikomos itin veiksmingomis, duomenų valdytojai turėtų įvertinti poveikį duomenų subjektų pagrindinėms teisėms bei laisvėms ir apsvarstyti, ar teisėto šių duomenų tvarkymo tikslo nebūtų galima pasiekti mažiau varžančiomis priemonėmis[37].

---

[32] Šie keturi Valdybos analizuojami scenarijai yra grindžiami Prašymo I priede nurodytais naudojimo atvejais. Prancūzijos PI paaiškino, kad prašymo I priede nurodyti naudojimo atvejai yra vaizdumo dėlei pateikiami su scenarijais susiję įgyvendinimo pavyzdžiai.

[33] 2012 m. balandžio 27 d. priimta 29 straipsnio duomenų apsaugos darbo grupės nuomonė Nr. 3/2012 dėl biometrinių technologijų pokyčių, WP193 (toliau – **29 straipsnio darbo grupės nuomonė Nr. 3/2012 dėl biometrinių technologijų**), p. 4. Pažymėtina, kad ši nuomonė yra susijusi su 1995 m. spalio 24 d. Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Duomenų apsaugos direktyva). Bendruoju duomenų apsaugos reglamentu buvo išplėsta specialių kategorijų duomenų taikymo sritis, kitaip nei Duomenų apsaugos direktyvoje nustatant, kad biometriniai duomenys yra specialių kategorijų duomenys (BDAR 9 straipsnis).

[34] Gairės dėl veido atpažinimo, Europos Tarybos konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu patariamasis komitetas, 2021 m. birželio mėn., p. 15; taip pat žr. EDAV gairių 05/2022 dėl veido atpažinimo teisėsaugos srityje 27 punktą.

[35] 29 straipsnio darbo grupės nuomonė Nr. 3/2012 dėl biometrinių technologijų, p. 29.

[36] EDAV gairių 05/2022 dėl veido atpažinimo teisėsaugos srityje 104 punktas.

[37] BDAR 39 konstatuojamoji dalis. Taip pat žr. EDAV gairių 3/2019 dėl vaizdo prietaisų 73 punktą.

28. Valdyba taip pat primena, kad teisė į asmens duomenų apsaugą nėra absoliuti ir pagal proporcingumo principą turėtų derėti su kitomis Chartija saugomomis pagrindinėmis teisėmis[38].

29. BDAR 25 straipsnio 1 dalyje nurodyti BDAR 5 straipsnyje išvardyti „duomenų apsaugos principai“[39] ir reikalaujama pritaikant priemones juos „veiksmingai“ įgyvendinti[40]. Šis reikalavimas aiškiai apima BDAR 5 straipsnio 1 dalies c punkte nustatytą duomenų kiekio mažinimo principą[41], pagal kurį reikalaujama, kad asmens duomenys būtų „adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi“, laikantis proporcingumo principo[42]. Be to, BDAR 25 straipsnio 2 dalyje nurodyta standartizuoto duomenų kiekio mažinimo prievolė ir nurodyta, kad ji taikoma surinktų asmens duomenų kiekiui, jų tvarkymo apimčiai, jų saugojimo laikotarpiui ir prieinamumui[43].

30. Vis dėlto BDAR 25 straipsnyje nereikalaujama, kad duomenų valdytojai įgyvendintų kokias nors konkrečias techninės ir organizacines priemones, veikiau reikalaujama, kad pasirinktos priemonės ir apsaugos priemonės būtų konkrečiai pritaikytos prie aplinkybių ir tvarkant duomenis duomenų subjektų teisėms ir laisvėms kylančių pavojų[44]. BDAR 32 straipsnyje dėl duomenų tvarkymo saugumo taip pat reikalaujama, kad duomenų valdytojai ir tvarkytojai įgyvendintų tinkamas techninės ir organizacines priemones, kad būtų užtikrintas pavojų fizinių asmenų teisėms ir laisvėms atitinkančio lygio saugumas.

31. Svarbu pažymėti tai, kad, net jei keleiviai aiškiai sutiktų su jų biometrinių duomenų naudojimu siekiant racionalizuoti keleivių srautus oro uostuose, Bendrajame duomenų apsaugos reglamente įtvirtinti su būtinumu ir proporcingumu susiję duomenų tvarkymo principai vis tiek taikomi ir jų reikia laikytis[45].

---

[38] BDAR 4 konstatuojamoji dalis. Šiuo atžvilgiu taip pat žr. 2021 m. birželio 22 d. Teisingumo Teismo sprendimo byloje *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504 (toliau – sprendimas byloje C-439/19 *Latvijas Republikas Saeima*), 98, 110 ir 113 punktus. Be to, pagal proporcingumo principą, kaip bendrąjį ES teisės principą, reikalaujama, kad Sąjungos aktais įgyvendinamos priemonės būtų tinkamos siekiamam tikslui įgyvendinti ir neviršytų to, kas būtina jam pasiekti (žr. 2010 m. lapkričio 9 d. Teisingumo Teismo sprendimo *Volker und Markus Schecke ir Eifert*, C-92/09 ir C-93/09, ECLI:EU:C:2010:662 (toliau – C-92/09 ir C-93/09 *Volker und Schecke*) 74 punktą ir jame nurodytą jurisprudenciją).

[39] 2020 m. spalio 20 d. priimtų EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 2.0 redakcijos (toliau – **EDAV gairės 4/2019 dėl pritaikytosios ir standartizuotos duomenų apsaugos**) 11 punktas.

[40] BDAR 25 straipsnio 1 dalyje nurodyta: „Atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas, tiek nustatydamas duomenų tvarkymo priemones, tiek paties duomenų tvarkymo metu, įgyvendina tinkamas techninės ir organizacines priemones, kaip antai pseudonimų suteikimą, kuriomis siekiama veiksmingai įgyvendinti duomenų apsaugos principus, kaip antai duomenų kiekio mažinimo principą, ir į duomenų tvarkymą integruoti būtinas apsaugos priemones, kad jis atitiktų šio reglamento reikalavimus ir apsaugotų duomenų subjektų teises.“ Taip pat žr. EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 13 punktą.

[41] BDAR 39 konstatuojamojoje dalyje atitinkamai nustatyta, kad asmens duomenys turėtų būti tvarkomi tik jei asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis.

[42] Sprendimo byloje C-439/19 *Latvijas Republikas Saeima* 98 punktas, 2019 m. gruodžio 11 d. Teisingumo Teismo sprendimo *Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (toliau – sprendimas byloje C-708/18 *M5A-ScaraA*) 48 punktas.

[43] EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 48 punktas.

[44] EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 14 punktas.

[45] EDAV gairių 5/2020 dėl sutikimo pagal Reglamentą 2016/679 5 punktas.

32. **Dėl būtinumo principo** Valdyba apsvarstys, ar siūlomo duomenų tvarkymo būtinai reikia siekiamam tikslui pasiekti ir ar tą patį tikslą taip pat veiksmingai galima pasiekti kitomis mažiau duomenų subjektų pagrindines teises ir laisves suvaržančiomis priemonėmis[46]. **Dėl proporcingumo principo** Valdyba vertins, ar neigiamas poveikis duomenų subjektų pagrindinėms teisėms ir laisvėms yra proporcingas numatytai naudai. Jei nauda yra palyginti maža, šis poveikis gali būti neproporcingas[47].

33. Bet kuriuo atveju, net jei Valdyba mano, kad kuris nors iš toliau analizuojamų scenarijų galėtų atitikti BDAR 5 straipsnio 1 dalies e bei f punktų ir 25 bei 32 straipsnių reikalavimus, duomenų valdytojas kiekvienu atveju tai turi įrodyti faktiniais elementais. Tai įrodant reikėtų atsižvelgti į alternatyvius scenarijus.

3.2 Dėl suderinamumo su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais

3.2.1 1 scenarijus. Užregistruoto biometrinio šablono saugojimas pas asmenį tapatybei patvirtinti

34. Šiame skirsnyje nagrinėjamas keleivių biometrinių šablonų saugojimo tik pas pačius asmenis, pvz., asmeniniuose jų prietaisuose[48], kuriuos tik jie kontroliuoja[49], tapatybės patvirtinimo tikslais[50] (toliau – **1 scenarijus**) suderinamumas su BDAR 5 straipsnio 1 dalies f punktu ir 25 bei 32 straipsniais. Šiame skirsnyje, atsižvelgiant į BDAR 25 ir 32 straipsnius, taip pat nagrinėjamos 1 scenarijui tinkamos apsaugos priemonės.

Scenarijaus aprašas

35. Pagal 1 scenarijų užregistruotas kiekvieno su šiuo duomenų tvarkymu sutikusio keleivio biometrinį šabloną saugo tik pats asmuo, pvz., tik paties keleivio kontroliuojamame asmeniniame prietaise. Keleivių tapatybė patvirtinama (atliekamas palyginimas „1 su 1“), kai jie oro uoste eina per konkrečius kontrolės punktus.

36. Registraciją atlieka oro uosto operatorius nuotoliniu būdu per savo programėlę[51] arba ji atliekama oro uostų terminaluose laikantis tinkamo tapatybės saugumo užtikrinimo lygio (pvz., tinkamo sistemos *eIDAS* saugumo užtikrinimo lygio[52]). Ši registracija apima duomenims tvarkyti reikiamo biometrinio šablono ir tapatybės duomenų[53] (toliau – **TD**) užregistravimą keleivio prietaise. Registracija atliekama

[46] Sprendimo byloje C-439/19 *Latvijas Republikas Saeima* 110 ir 113 punktai, 2023 m. liepos 4 d. Teisingumo Teismo (didžiosios kolegijos) sprendimo byloje *Meta / Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537 108 punktas.

[47] Sprendimo byloje C-708/18 *M5A-ScaraA* 52–56 punktai, sprendimo bylose C-92/09 ir C-93/09 *Volker und Schecke* 87 punktas, sprendimo byloje C-439/19 *Latvijas Republikas Saeima* 98 110 ir 113 punktai. Taip pat žr. 29 straipsnio darbo grupės nuomonę 3/2012 dėl biometrinių technologijų, p. 8.

[48] Asmuo savo biometrinį šabloną taip pat galėtų išspausdinti ir saugoti popieriuje.

[49] Tai nedaro poveikio bendrajai su duomenų tvarkymu susijusiai duomenų valdytojo atsakomybei.

[50] Kaip nurodyta Prašymo I priede aprašant 1 naudojimo atvejį.

[51] EDAV atkreipia dėmesį į tai, kad ateityje būtų galima numatyti alternatyvius šio registravimo būdus, registraciją galbūt atliekant ne specialia oro uosto operatoriaus programėle, bet, pvz., naudojantis sąveika su naudotojo skaitmenine dėkle.

[52] Elektroninės atpažinties ir patikimumo užtikrinimo paslaugų sistema (toliau – ***eIDAS***) grindžiama 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentu (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu.

[53] Šioje nuomonėje tapatybės duomenimis vadinami tokie duomenys kaip pavardė, vardas, gimimo data ir pan., kurie, patikrinus juos pagal asmens dokumentą arba pasą, buvo nustatyti kaip tikslūs.

tik vieną kartą konkrečiam galiojimo laikotarpiui (pvz., jis gali atitikti keleivio paso galiojimo laikotarpį). Užbaigus registraciją, oro uosto operatorius neišsisaugo nei keleivio TD, nei jo biometrinių duomenų.

37. Konkrečiai dėl saugojimo pažymėtina, kad keleivio TD ir biometrinis šablonas yra saugomi vietoje kiekvieno keleivio prietaise (pvz., mobiliojoje oro uosto operatoriaus programėlėje arba skaitmeninės dėklės programėlėje). Paskui naudojantis prietaisu galima perduoti keleivio TD arba biologinį šabloną, galbūt taip pat skrydžio informaciją ir (arba) Įlaipinimo taloną, arba teikti užklausas dėl jų. Pavyzdžiui, ši informacija užšifruojama raktu, kurį turi tik oro uosto operatorius, – galbūt užkoduota kaip QR kodas, kurį galima išspausdinti popieriuje arba parodyti keleivio prietaiso ekrane. Tada šiuo atveju keleivis parodytų šį QR kodą specialiems oro uoste esantiems kontrolės aparatams, kuriuose įrengti QR skaitytuvai ir kameros.

38. Saugumo atžvilgiu pažymėtina, kad atitikties nustatymo metu QR kodai iššifruojami raktu, kurį turi oro uosto operatorius, – iššifruoti QR kodus gali tik jis. Keleivio biometriniai duomenys laikomi tik trumpą laikotarpį, o užbaigus atitikties nustatymą ištrinami. Pažymėtina, kad su saugojimu susijusios saugumo priemonės iš dalies priklauso nuo keleivio prietaiso saugumo.

EDAV vertinimas

39. Pagal 1 scenarijų aprašytos BDAR 5 straipsnio 1 dalies f punkte ir 32 straipsnyje reikalaujamos techninės ir organizacinės priemonės, kuriomis siekiama užtikrinti duomenų subjektams kylančius pavojus atitinkančio lygio saugumą. Keleivių tapatybė patvirtinama (atliekamas palyginimas „1 su 1“), kai jie oro uoste eina per konkrečius kontrolės punktus. Pagal šį scenarijų pagrindinė atitikties nustatymo operacija atliekama kontroliuojamoje aplinkoje[54], kurioje keleiviai aktyviai dalyvauja ir gali labiau kontroliuoti savo duomenis. Visų pirma, būtų tikrinami tik su šiuo duomenų tvarkymu sutikę keleiviai, ir, kadangi jie būtų tikrinami prie specialių aparatų, kitų dėl šio duomenų tvarkymo sutikimo nedavusių keleivių biometriniai duomenys nebūtų renkami. Be to, sutikę keleiviai turi galimybę šį duomenų tvarkymą bet kada sustabdyti, ištrindami duomenis iš savo prietaisų.

40. Veido atpažinimo naudojimas pagal biometrinį šabloną, kurį saugo tik pats asmuo, pvz., tik jo(s) kontroliuojamame asmeniniame prietaise, ir kuris per specialią sąsają naudojamas tapatybei patvirtinti konkrečiuose kontrolės punktuose, tam tikromis sąlygomis kelia mažiau pavojų nei centralizuotoje duomenų bazėje saugomų biometrinių duomenų naudojimas[55]. Taip saugant duomenis vietoje ir kartu taikant tinkamas apsaugos priemones[56], sumažinamas asmens duomenų pažeidimų sunkumas, kiek tai susiję su nukentėjusiųjų asmenų skaičiumi, palyginti su centralizuotu saugojimu, ir užtikrinamas aktyvus duomenų subjektų dalyvavimas suteikiant prieigą prie biometrinių šablonų.

41. Be to, nustatyti atitiktį būtų galima vietoje, oro uoste, biometrinį šabloną, pvz., pateiktą QR kode, lyginant su šablono rezultatu, apskaičiuotu remiantis kontrolės aparato kamera užfiksuotu biometrinių duomenų pavyzdžiu. Konkretų patikrinimą atliekantis duomenų valdytojas (jis galėtų būti oro uosto

[54] Sąvoka „nekontroliuojama aplinka“ vartojama naudojant veido atpažinimą tapatybei nustatyti, kai duomenų subjektai aktyviai nedalyvauja, o kiekvieno į stebėjimo zoną patenkančio veido šablonas lyginamas su duomenų bazėje saugomais didelės gyventojų grupės šablonais, – žr. EDAV gairių 05/2022 dėl veido atpažinimo teisėsaugos srityje 17 punktą.

[55] EDAV gairių 05/2022 dėl veido atpažinimo teisėsaugos srityje 17 punktas.

[56] Kaip aprašyta toliau nuo 46 punkto.

operatorius arba oro transporto bendrovė, atsižvelgiant į tai, kur – oro uosto saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir (arba) patekimo į keleivių laukiamuosius vietose – šis patikrinimas atliekamas) sužinotų ir naudotų tik atitikties nustatymo rezultatą. Be to, tai, kad atitikčiai nustatyti reikiamą informaciją (pvz., QR kodą) turi pateikti asmuo, yra antrasis veiksnys[57], o tai padidina tapatybės patvirtinimo saugumą.

42. Atsižvelgiant į BDAR 25 straipsnį, ypač siekiant laikytis duomenų kiekio mažinimo reikalavimo, reikėtų užtikrinti, kad duomenų tvarkymas atitiktų būtinumo principą. Pagal 1 scenarijų pasirinktos priemonės galėtų būti laikomos atitinkančiomis būtinumo principą, atsižvelgiant į siekiamą tikslą (t. y. keleivių srauto racionalizavimas), jei, atsižvelgdamas į duomenų tvarkymo aplinkybes, duomenų valdytojas gali įrodyti, kad nėra alternatyvių mažiau varžančių sprendimų, kuriais tą patį tikslą būtų galima pasiekti taip pat veiksmingai. Pavyzdžiui, duomenų valdytojas gali sugebėti įrodyti, kad, net jei keleiviai turėtų parodyti savo prietaisą, pagal 1 scenarijų patikrinimo procesas vyktų greičiau nei dabar, kai patikrinimą, ar įlaipinimo talone nurodyti vardas ir pavardė atitinka nurodytuosius keleivio asmens dokumente[58], atlieka žmogus. To nebūtų galima įrodyti ypač tais atvejais, kai keleivių tapatybė pagal oficialius asmens dokumentus šiuo metu netikrinama (šiuo atžvilgiu žr. pirmiau išdėstytą 18 punktą).

43. Be to, po registracijos biometrinių šablonų oro uosto operatorius nelaiko pas save, o laikotarpis, kai patikrinimą atliekantis duomenų valdytojas turi biometrinius duomenis, yra labai trumpas, nes šie duomenys ištrinami iškart, kai tik užbaigiamas atitikties nustatymas. Todėl atrodo, kad pagal 1 scenarijų pasirinktomis priemonėmis sumažinamas duomenų tvarkymo mastas ir asmens duomenų saugojimo laikotarpis.

44. Proporcingumo principo atžvilgiu pažymėtina, kad varžomąjį šio duomenų tvarkymo poveikį galima sumažinti aktyviu keleivių dalyvavimu, nes savo biometrinius duomenis saugotų tik jie patys. Be to, atsižvelgiant į pirmiau aprašytas priemones ir darant prielaidą, kad duomenų valdytojas įgyvendina tinkamas apsaugos priemones, kurių reikalaujama dėl konkretaus nagrinėjamo duomenų tvarkymo, įgyvendinus tinkamas priemones būtų galima užtikrinti pavojų atitinkančio lygio saugumą. Šiuo atveju neigiamas poveikis duomenų subjektų pagrindinėms teisėms ir laisvėms galėtų būti laikomas proporcingu numatytai naudai.

45. Todėl, atsižvelgdama į tai, kas išdėstyta pirmiau, atsakydama į 1.1 klausimą Valdyba daro išvadą, kad šis duomenų tvarkymas **iš esmės galėtų būti laikomas suderinamu su BDAR 5 straipsnio 1 dalies f punktu, 25 ir 32 straipsniais, jei būtų taikomos tinkamos apsaugos priemonės**.

Tinkamos apsaugos priemonės

46. Atsakydama į 1.2 klausimą, EDAV mano, kad pagal tokį scenarijų turėtų būti įgyvendinamos bent toliau nurodytos apsaugos priemonės. Siekiant įgyvendinti tuos pačius saugumo ir duomenų apsaugos tikslus, galėtų būti taikomos kitos nei šioje nuomonėje aprašytos apsaugos priemonės. Jos galėtų būti teisėtos, jei jomis užtikrinama atitiktis taikomai teisinei sistemai.

[57] Pavyzdžiui, taip sumažėja rizika, kad bus apsimetama kitu asmeniu. Taip pat žr. toliau nurodytą C.1.2 apsaugos priemonę.
[58] Taip pat būtų galima argumentuoti, kad atliekant biometrinį patikrinimą padaroma mažiau klaidų nei žmogaus atliekamo patikrinimo atveju.

47. Pastaba. Tai bendra ir neišsami galimų tinkamų apsaugos priemonių, kurias turėtų įgyvendinti į 1 scenarijų panašų sprendimą pasirinkęs taikyti duomenų valdytojas, apžvalga. Šių priemonių tinkamumas pagal BDAR 25 ir 32 straipsnius priklausys nuo konkretaus atvejo analizės. Visi duomenų valdytojai turės užtikrinti, kad būtų atliktas jų pačių poveikio duomenų apsaugai vertinimas (toliau – PDAV)[59], o konkretiems jų sprendimams gali prireikti papildomų į šią nuomonę neįtrauktų priemonių.

A. Bendrieji aspektai

A.1. Duomenų tvarkymo poveikio vertinimas

A.1.1. Atlikti PDAV laikantis BDAR 35 straipsnio reikalavimų, jei duomenų valdytojas planuoja naują duomenų tvarkymo operaciją, susijusią su duomenų tvarkymu, dėl kurio gali kilti didelis pavojus . Taip tikriausiai bus pagal 1 scenarijų, nes pagal jį biometriniai duomenys tvarkomi dideliu mastu[60]. Ankstyvame veido atpažinimo sistemos kūrimo etape įvertinti jos įgyvendinimo tinkamumą, įskaitant jos būtinumą ir proporcingumą siekiamų tikslų atžvilgiu[61], ir visą produkto plėtros gyvavimo laikotarpį atlikti jos peržiūrą.

A.1.2. Konsultuotis su susijusia priežiūros institucija, jei dėl duomenų tvarkymo vis dar kyla didelis pavojus, nors duomenų valdytojas ėmėsi priemonių šiam pavojui sumažinti[62].

A.2. Duomenų subjektų teisės ir apsaugos priemonės, kurias gali įgyvendinti duomenų valdytojai

A.2.1. Apsaugos priemonės, kuriomis būtų galima atsižvelgti į klaidingai neigiamus rezultatus. Mažinti šališkumo dėl amžiaus, lyties ir rasės pavojų „reguliariai vertinant, ar algoritmai veikia pagal paskirtį, ir tikslinant algoritmus siekiant sumažinti atskleistus šališkumus ir užtikrinti sąžiningą duomenų tvarkymą“[63]. Pavyzdžiui, nustatyti žmogaus atliekamą priežiūrą ir žmogaus įsikišimą, siekiant sumažinti šališkumą ir užtikrinti kad keleiviai nebūtų stigmatizuojami arba profiliuojami.

A.2.2. Užtikrinti, kad visas asmens duomenų tvarkymas būtų skaidrus, o asmenys būtų informuoti ir galėtų kontroliuoti, kaip jų duomenys tvarkomi atliekant kiekvieną duomenų tvarkymo operaciją[64].

[59] BDAR 35 straipsnis.
[60] BDAR 35 straipsnio 3 dalis ir 2017 m. spalio 13 d. priimtos, EDAV patvirtintos 29 straipsnio darbo grupės Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų, WP 248, 1-oji peržiūrėta redakcija.
[61] BDAR 35 straipsnio 7 dalies b punktas.
[62] BDAR 36 straipsnio 1 dalis.
[63] EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 60 išnaša ir 70 punktas.
[64] EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 68 punktas ir BDAR 7 konstatuojamoji dalis.

A.2.3. Užtikrinti, kad būtų taikomos priemonės, siekiant laikytis tikslo apribojimo principo, kad duomenys nebūtų naudojami kitais, pvz., saugumo arba mokymo, tikslais.

A.2.4. Tinkamomis priemonėmis užtikrinti, kad nebūtų daromos su veido atpažinimu nesutinkančių asmenų nuotraukos arba vaizdo įrašai, net jei jie nėra įrašomi ir tvarkomi (pvz., taikant tinkamą lauko gylį ir fiksavimo sritį, kad nebūtų fiksuojami kitų fone arba aplinkui esančių keleivių atvaizdai, taikant specialias eiles, kurios būtų aiškiai pažymėtos kaip veido atpažinimo eilės).

A.2.5. Jei tuos pačius aparatus gali naudoti ir su veido atpažinimu sutinkantys, ir su juo nesutinkantys keleiviai arba jei tuo metu, kai sistema nenaudojama, matymo lauke gali pasirodyti keleivių, kurie nesutinka su veido atpažinimu, prieš pradedant daryti nuotrauką arba vaizdo įrašą palaukti, kol sutinkantis keleivis atliks tai patvirtinantį veiksmą.

A.2.6. Suteikti duomenų subjektui galimybę bet kuriuo metu ištrinti tik pas jį mobiliojoje programėlėje arba skaitmeninėje dėklėje esančius duomenis (biometrinį šabloną[65])[66].

A.2.7. Nustatyti tinkamas alternatyvas arba atsarginius sprendimų variantus (t. y. keleiviams, kurie nesutiktų su jų biometrinių duomenų naudojimu, negalėtų naudotis šiais sprendimais arba būtų klaidingai atmesti), taip pat siekiant užtikrinti, kad nesutinkantys keleiviai nepatirtų jokių pasekmių[67].

A.2.8. Jei naudojama programėlė, ji turėtų būti atidžiai sukurta ir sukonfigūruota taip, kad nebūtų renkami nereikalingi duomenys ir nereikėtų naudoti trečiųjų šalių programavimo komplektų (toliau – PK), kuriais duomenys būtų renkami kitais tikslais.

A.3. Atskaitomybė

A.3.1. Išsiaiškinti, ar esama susijusių elgesio kodeksų arba sertifikavimo mechanizmų, pagal kuriuos būtų lengviau įrodyti, kad laikomasi BDAR 32 straipsnyje nustatytų duomenų tvarkymo saugumo reikalavimų[68]. Patikrinti priemonių tinkamumą atliekant konkretų nagrinėjamą duomenų tvarkymą. Nustatant, kokios priemonės yra tinkamos, gali būti naudingi asociacijų ir kitų įstaigų, atstovaujančių tam tikrų kategorijų duomenų valdytojams, pripažinti standartai[69], geriausia praktika ir elgesio kodeksai.

A.3.2. Prieš leidžiant pradėti registracijos etapą, užtikrinti, kad naudotojų prietaisuose būtų atlikti pagrindiniai saugumo patikrinimai, net jei keleiviai taip pat turi atsakomybę už savo

[65] 1 scenarijui skirtų apsaugos priemonių nuorodos į biometrinį šabloną atitinka 2 scenarijaus nuorodas į raktą ir (arba) slaptažodį.
[66] Pažymėtina, kad ši apsaugos priemonė taikoma tik 1 scenarijui.
[67] EDAV gairių 3/2019 dėl vaizdo prietaisų 86 punktas.
[68] BDAR 32 straipsnio 3 dalis ir EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 10 punktas.
[69] Žr., pvz., ISO/IEC 2382-37.

duomenų, kai jie saugomi jų prietaisuose, apsaugą. Tokių techninių patikrinimų ir kontrolės pavyzdžių pateikta toliau C.2 skirsnyje „Infrastruktūra ir tinklas“.

B. Organizaciniai aspektai

B.1. Politika ir atitiktis

B.1.1. Užtikrinti, kad būtų vykdoma vidaus prieigos kontrolė[70] ir būtų nustatytos administratoriams taikomos taisyklės.

B.1.2. Jei veido atpažinimo paslaugą gali teikti viena iš duomenų tvarkymo veikloje dalyvaujančių šalių, o kitoms dalyvaujančioms šalims tvarkyti tapatybės, biometrinių arba abiejų šių rūšių duomenų nereikia, uždrausti šių duomenų srautą per šias kitas trečiąsias šalis. Pavyzdžiui, bendra oro uosto infrastruktūra besinaudojančiai oro transporto bendrovei nereikia techninės prieigos prie biometrinių duomenų, net jei pagal BDAR tvarkydama duomenis ji veikia kaip duomenų valdytoja.

B.1.3. Nustatyti šifravimo ir raktų valdymo politiką[71], pvz., taikomą TD ir biometrinių duomenų tvarkymui.

B.1.4. Užtikrinti atitiktį BDAR V skyriui. Pavyzdžiui, užtikrinti reikalavimus atitinkantį perdavimą, jei duomenų valdytojas registracijos metu naudojasi trečiojoje valstybėje teikiama nuotoline paslauga.

B.1.5. Jei naudojamasi duomenų tvarkytojų paslaugomis, užtikrinti, kad būtų taikomas BDAR 28 straipsnio 3 dalyje nurodytas susitarimas su duomenų tvarkytoju[72].

B.1.6. Užtikrinti, kad būtų taikomos procedūros, kuriomis būtų valdoma žmogaus atliekama priežiūra ir įsikišimas, ypač sprendžiant klaidingo atmetimo ir techninius arba naudojimosi galimybių klausimus.

B.2. Mokymas ir testavimas

B.2.1. Užtikrinti, kad darbuotojai būtų tinkamai mokomi.

B.2.2. Įgyvendinti „reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą“[73].

[70] 2020 m. balandžio 21 d. priimtos EDAV gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių naudojimo COVID-19 protrūkio aplinkybėmis (toliau – **EDAV gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išsiaiškinimo priemonių**), SEC-10, p. 16.
[71] EDAV gairių 3/2019 dėl vaizdo prietaisų 89 punktas.
[72] BDAR 28 straipsnio 3 dalis.
[73] BDAR 32 straipsnio 1 dalies d punktas.

B.2.3. Įgyvendinti procesą, kuriuo būtų užtikrinta, kad keleivių biometrinių šablonų[74] tvarkymas tapatybei patvirtinti techniniu požiūriu būtų veiksmingas ir pakankamai tikslus.

B.2.4. Užtikrinti, kad registruojantis ir kontrolės punktuose surinkti biometrinių duomenų pavyzdžiai būtų pakankamai kokybiški, kad būtų galima atlikti patikimą biometrinių duomenų tvarkymą.

C. Techniniai aspektai

C.1. Prieiga

C.1.1. Įgyvendinti registracijos etapu taikytinas apsaugos priemones, siekiant užtikrinti saviranka grindžiamą registraciją remiantis patikrinta tapatybe. Pavyzdžiui, siekiant pagerinti daugiaveiksnio naudotojų tapatybės patvirtinimo vertinimą, galima įgyvendinti įvairius veiksmus: nuo slaptažodžiais apsaugotų vienkartinių nuorodų, kuriomis galima suaktyvinti programėlę, iki vietoje taikomų prietaisų atblokavimo mechanizmų.

C.1.2. Įgyvendinti apsaugos priemones, kuriomis būtų galima atsižvelgti į klaidingai teigiamus rezultatus, užkirsti kelią apsimetinėjimui ir sukčiavimui[75].

C.1.3. Uždrausti bet kokią išorinę prieigą prie TD ir biometrinių duomenų[76].

C.1.4. Užtikrinti, kad duomenų tvarkymas registracijos, perdavimo ir atitikties nustatymo etapuose būtų atliekamas vietoje. Atitikties nustatymo punktas turėtų būti kuo arčiau asmens prietaiso. Kad šablono atitiktį būtų galima nustatyti asmeniniame prietaise, gali prireikti sąveikos su paslaugų teikėjais, kurie yra ne oro uoste, ir naudotis viešojo tinklo ištekliais, o tai yra trūkumas, nes daromas poveikis pasiekiamumui, o šablonas platinamas išorės subjektams.

C.1.5. Nustatyti naudotojo tapatumą, kad būtų galima pridėti naują skrydį ir sukurti naują šifruotą QR kodą.

C.1.6. Įgyvendinti priemones siekiant atsižvelgti į atvejį, kai keleivis gali prarasti prieigą prie savo QR kodo.

C.2. Infrastruktūra ir tinklas

C.2.1. Operacinei sistemai (toliau – OS) taikomos sąlygos, kad ji būtų naujinama ir būtų įjungta tapatybės patvirtinimo funkcija, norint gauti prieigą prie prietaiso, kad programėlė ir (arba)

[74] 1 scenarijui skirtų apsaugos priemonių nuorodos į biometrinį šabloną atitinka 2 scenarijaus nuorodas į raktą ir (arba) slaptažodį.
[75] 2022 m. sausio mėn. ENISA ataskaita *Digital Identity. Leveraging the Self-Sovereign Identity (SSI). Concept to Build Trust* (liet. „Skaitmeninė tapatybė. Naudojimasis nepriklausomos tapatybės galimybėmis. Pasitikėjimo didinimo koncepcija“).
[76] EDAV gairių 3/2019 dėl vaizdo prietaisų 89 punktas.

skaitmeninė dėklė galėtų veikti, įskaitant automatinį TD ir biometrinių duomenų ištrynimą, jei OS yra pasenusi ir kelia saugumo pavojų.

C.2.2. Veikimo metu izoliuoti prie tinklo prijungtus atitikties nustatymo įrenginius (t. y. kontrolės aparatus) ir imtis visų kitų reikiamų saugumo užtikrinimo priemonių.

C.2.3. Atlikti biometrinį atitikties nustatymą keleivio prietaise arba kontrolės aparate (tinklo paribio kompiuterija).

C.2.4. Sprendimai, kuriais būtų galima pašalinti su saugumu susijusį keleivių individualių prietaisų pažeidžiamumą, įskaitant (bent) nenaudojamų biometrinių ir tapatybės duomenų šifravimą.

C.2.5. Naudoti saugią tik naudotojo turimą (bent) biometrinių duomenų[77] saugyklą, pvz., saugią sritį (ang. *secure enclave*) išmaniajame telefone.

C.2.6. Saugumo apsaugos priemonės fiziniam patalpų, įskaitant oro uosto biometrinių duomenų terminalą, saugumui užtikrinti. Užtikrinti labai didelį TD ir biometrinių duomenų tvarkymo struktūros elementų (pvz., skaičiavimo, duomenų srauto, pereinamojo laikotarpio arba ilgalaikio saugojimo) saugumą.

C.3. Naudotojų tapatybės patikros duomenų saugumas ir valdymas

C.3.1. Užtikrinti, kad perduodami ir saugomi duomenys būtų suskirstyti bent į tris skirtingas grupes, pvz., TD, biometriniai duomenys ir skrydžio informacija[78]. Užtikrinti, kad nuo perdavimo iki saugojimo duomenys būtų tinkamai užšifruojami.

C.3.2. Taikyti technines priemones, siekiant užtikrinti, kad kontrolės punkte būtų tvarkomi ir tikrinami tik tie duomenys, kuriuos galima teisėtai tvarkyti konkrečiuose kontrolės punktuose.

C.3.3. Užtikrinti duomenų ištrynimo veiksmingumą[79], taikant saugią ištrynimo procedūrą (pvz., pagrindinę atmintinę, podėliavimą, galimas atsargines kopijas), ir įvertinti, kada duomenų ištrynimas turėtų būti automatizuotas. Duomenų saugojimo laikotarpių laikymasis turėtų būti griežtai užtikrinamas automatinėmis procedūromis, kad asmenims nereikėtų imtis papildomų veiksmų[80].

C.3.4. Užtikrinti duomenų (pvz., parašo) autentiškumą ir vientisumą[81].

[77] 1 scenarijui skirtų apsaugos priemonių nuorodos į biometrinį šabloną atitinka 2 scenarijaus nuorodas į raktą ir (arba) slaptažodį
[78] EDAV gairių 3/2019 dėl vaizdo prietaisų 89 punktas.
[79] EDAV gairių 3/2019 dėl vaizdo prietaisų 89 punktas.
[80] EDAV gairių 4/2019 dėl 25 straipsnio „Pritaikytoji ir standartizuotoji duomenų apsauga“ 82 punktas.
[81] EDAV gairių 3/2019 dėl vaizdo prietaisų 89 punktas.

C.3.5. Keleivių biometrinius duomenis registracijos ir kontrolės punktuose laikyti tik labai trumpai ir ištrinti, kai tik keleivis pereina per kontrolės punktą.

C.3.6. Jei registracijai naudojama programėlė, ją kuriant taikyti mobiliųjų programėlių saugumo standartus ir pavesti išbandyti jos saugumą trečiajai šaliai.

C.3.7. Užtikrinti, kad per registravimo etapą oro uoste būtų taikomos saugumo priemonės, siekiant išsaugoti keleivių biometrinių duomenų konfidencialumą ir vientisumą. Pavyzdžiui, jei QR kodą išspausdina terminalo darbuotojai, jis terminale neturėtų būti rodomas, kad niekas negalėtų jo piktavališkai nufotografuoti. Mažojo nuotolio perdavimo atvejais perdavimas turėtų būti atliekamas remiantis aktyviu naudotojo dalyvavimu ir per tokį kanalą, kuriuo užtikrinamas artumas.

C.3.8. Tik asmens turimi duomenys[82] turėtų būti laikomi saugioje saugykloje asmeniniame prietaise, o visam galimam su prietaiso operacinėmis sistemomis susijusiam pažeidžiamumui turi būti taikomos tinkamos saugumo pataisos. Jei naudojamas išspausdintas QR kodas, asmenį reikėtų informuoti apie itin neskelbtiną jame pateiktų duomenų pobūdį ir apie tai, ką su jais galima atlikti.

C.3.9. Užtikrinti, kad registracija būtų atliekama taikant tinkamus nuotolinio tapatybės įrodymo metodus[83].

3.2.2 2 scenarijus. Centralizuotas užregistruotų biometrinių šablonų saugojimas šifruota forma oro uoste tapatybei patvirtinti, kai raktus ir (arba) slaptažodžius turi tik keleiviai

48. Šiame skirsnyje nagrinėjamas centralizuoto užregistruotų keleivių biometrinių šablonų saugojimo šifruota forma centralizuotoje duomenų bazėje tapatybei patvirtinti, kai raktus ir (arba) slaptažodžius turi tik keleiviai[84], (toliau – **2 scenarijus**) suderinamumas su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais. Šiame skirsnyje, atsižvelgiant į BDAR 25 ir 32 straipsnius, taip pat nagrinėjamos 2 scenarijui tinkamos apsaugos priemonės.

Scenarijaus aprašas

49. Pagal 2 scenarijų registracija atliekama tik vieną kartą konkrečiam galiojimo laikotarpiui (pvz., vienus metus nuo paskutinio skrydžio iki paso galiojimo pabaigos datos) nuotoliniu būdu, laikantis tinkamo tapatybės saugumo užtikrinimo lygio (pvz., tinkamo sistemos *eIDAS* saugumo užtikrinimo lygio), arba oro uostų terminaluose. Registraciją valdo oro uosto operatorius, o jos metu sugeneruojami TD ir biometriniai duomenys, kurie yra užšifruojami raktu ir (arba) slaptažodžiu.

50. Duomenų bazė saugoma oro uosto patalpose oro uosto operatoriaus žinioje. Konkrečiam asmeniui skirti šifravimo raktai ir (arba) slaptažodžiai saugomi tik to asmens prietaise (pvz., mobiliojoje oro

[82] 1 scenarijui skirtų apsaugos priemonių nuorodos į biometrinį šabloną atitinka 2 scenarijaus nuorodas į raktą ir (arba) slaptažodį.
[83] Žr. ENISA ataskaitą *Report on Remote ID Proofing: Analysis of methods to carry out identity proofing remotely* (liet. „Ataskaita dėl nuotolinio tapatybės įrodymo. Nuotolinio tapatybės įrodymo metodų analizė“), 2021 m.
[84] Remiantis Prašymo I priede pateiktu 2 naudojimo atvejo pavyzdžiu.

uosto operatoriaus programėlėje). Programėle galima sugeneruoti QR kodą, į kurį įtrauktas raktas ir (arba) slaptažodis ir kurį galima išspausdinti popieriuje arba parodyti prietaiso ekrane[85]. Be to, oro uosto operatorius savo žinioje esančiais raktais atlieka antrojo lygmens šifravimą[86].

51. Keleivių tapatybė patvirtinama (atliekamas palyginimas „1 su 1“), kai jie oro uoste eina per specialius kontrolės punktus. Nusprendę eiti per biometrinių duomenų kontrolės punktus keleiviai parodo savo QR kodus specialiam kontrolės aparatui, kuriame įrengtas QR skaitytuvas ir kamera. Keleivio indeksas siunčiamas į duomenų bazę, kad būtų galima pateikti užklausą dėl šifruoto šablono, kuris atsiunčiamas ir tikrinamas vietoje kontrolės aparate ir (arba) naudotojo prietaise. Kontrolės punkte dirbantis duomenų valdytojas sužino ir naudoja tik atitikties nustatymo rezultatą[87].

52. Pagal šį scenarijų TD ir biometrinių duomenų srautų tarp oro uostų nevyksta, o centralizuotos duomenų bazės nėra nei tarpusavyje susietos, nei sąveikios.

EDAV vertinimas

53. Pagal 2 scenarijų užregistruoti keleivių biometriniai šablonai saugomi centralizuotai, bet šifruota forma, o raktus ir (arba) slaptažodžius turi tik keleiviai. Pagal 2 scenarijų keleivių tapatybė yra patvirtinama (atliekamas palyginimas „1 su 1“).

54. Pagal šį scenarijų keleivių srauto racionalizavimo tikslo (t. y. spartesnės kontrolės) siūloma siekti naudojant centralizuotą sistemą. Anksčiau EDAV buvo atkreipusi dėmesį į tai, kad šis sprendimas galėtų būti laikomas perspektyvia alternatyva decentralizuotam užregistruotų biometrinių šablonų saugojimui[88] (kaip aprašyta pagal 1 scenarijų), jei esama objektyvių poreikių ir taikomos tinkamos apsaugos priemonės (žr. toliau nuo 60 punkto aprašytas apsaugos priemones).

55. Dėl saugumo pažymėtina, kad kiekvieno asmens duomenys yra užšifruojami specialiu tik asmens turimu ir tik jo kontroliuojamu raktu. Be to, tai, kad atitikčiai nustatyti reikiamą informaciją (t. y. slaptažodį ir (arba) kodą) turi pateikti asmuo, yra antrasis veiksnys[89], o tai padidina tapatybės patvirtinimo saugumą. Be to, oro uosto operatorius savo žinioje esančiais raktais atlieka antrojo lygmens šifravimą. Pagal 2 scenarijų asmens indeksas siunčiamas į centrinę duomenų bazę, siekiant gauti su asmeniu susijusius biometrinius duomenis. Tada šie duomenys (šifruota forma) siunčiami į kompiuterį kontrolės punkte, kur jie iššifruojami, siekiant nustatyti atitiktį, o patikrinimą kontrolės punkte atliekantis duomenų valdytojas sužino tik atitikties nustatymo rezultatą. Todėl, jei asmens raktas ir (arba) slaptažodis laikomas kontrolės punkte esančiame kompiuteryje, o į centrinę duomenų bazę, siekiant gauti šifruotą biometrinį šabloną, siunčiamas tik keleivio indeksas, šias saugumo priemones būtų galima laikyti suderinamomis su BDAR 5 straipsnio 1 dalies f punktu ir 32 straipsniu.

[85] Prancūzijos PI taip pat paaiškino, kad gali būti kitų techninių reikiamos informacijos siuntimo sprendimų, pvz., taikant mažojo nuotolio ryšio protokolą.
[86] Pats raktas ir (arba) slaptažodis (kuris yra pas asmenį) yra užšifruojamas dar vienu raktu, kurį turi oro uosto operatorius.
[87] Prancūzijos PI paaiškino, kad šis saugojimo laikotarpis nurodytas tik kaip pavyzdys ir gali būti laikomas tinkamu, nes raktai yra pas asmenis, ir gali būti pasirenkamas registravimosi etape. Vis dėlto pažymėtina, kad šis saugojimo laikotarpis gali būti keičiamas.
[88] EDAV gairių 3/2019 dėl vaizdo prietaisų 88 punktas.
[89] Pavyzdžiui, taip sumažėja rizika, kad bus apsimetama kitu asmeniu. Taip pat žr. C.1.2 apsaugos priemonę.

56. Atsižvelgiant į BDAR 25 straipsnį, ypač siekiant laikytis duomenų kiekio mažinimo reikalavimo, reikėtų užtikrinti, kad duomenų tvarkymas atitiktų būtinumo principą. Pagal 2 scenarijų pasirinktos priemonės galėtų būti laikomos atitinkančiomis būtinumo principą, atsižvelgiant į siekiamą tikslą (t. y. keleivių srauto racionalizavimo oro uostuose), jei, atsižvelgdamas į duomenų tvarkymo aplinkybes, duomenų valdytojas gali įrodyti, kad nėra alternatyvių mažiau varžančių sprendimų, kuriais tą patį tikslą būtų galima pasiekti taip pat veiksmingai. Pagal 2 scenarijų keleiviai vis tiek turėtų parodyti savo prietaisą[90]. Vis dėlto duomenų valdytojas gali turėti galimybę įrodyti, kad pagal 2 scenarijų patikrinimo procesas vyktų greičiau nei dabar, kai patikrinimą, ar įlaipinimo talone nurodyti vardas ir pavardė atitinka nurodytuosius keleivio asmens dokumente[91], atlieka žmogus, arba palyginti su 1 scenarijumi. To nebūtų galima įrodyti ypač tais atvejais, kai keleivių tapatybė pagal oficialius asmens dokumentus šiuo metu netikrinama (šiuo atžvilgiu žr. pirmiau išdėstytą 18 punktą).

57. Dėl proporcingumo principo pažymėtina, kad varžomąjį šio duomenų tvarkymo poveikį galima sumažinti aktyviai dalyvaujant keleiviams, kurie tik patys kontroliuoja šifruotiems jų duomenims skirtus raktus. Be to, atrodo, kad su keleivių biometrinių duomenų saugojimu centralizuotoje duomenų bazėje, kai raktus turi tik keleiviai, susijusius pavojus saugumui galima sumažinti taikant tinkamas apsaugos priemones (žr. toliau nuo 60 punkto aprašytas apsaugos priemones). Todėl, darant prielaidą, kad duomenų valdytojas įgyvendina tinkamas apsaugos priemones, kurių reikia dėl nagrinėjamo konkretaus duomenų tvarkymo, asmenims kylantys pavojai galėtų būti sumažinami, o neigiamas poveikis duomenų subjektų pagrindinėms teisėms ir laisvėms galėtų būti laikomas proporcingu numatytai naudai. Žinoma, kiekvienu atveju reikėtų užtikrinti, kad būtų tvarkomi tik tie duomenys, kurių tuo tikslu reikia, ir kad būtų tikrinami tik sutikimą davę keleiviai, todėl nekyla pavojus, kad bus renkami kitų sutikimo nedavusių keleivių biometriniai duomenys.

58. Prašyme nurodyta, kad, pvz., pagal 2 scenarijų šifruotų duomenų saugojimo duomenų bazėje laikotarpis paprastai galėtų trukti vienus metus nuo paskutinio asmens skrydžio iki paso galiojimo pabaigos datos. Prašyme nepateikta informacijos, kuria toks ilgas laikotarpis būtų pagrįstas objektyviomis priežastimis, nors galima daryti prielaidą, kad toks saugojimo laikotarpis numatytas, kad būtų patogiau skrendant ateityje. Dėl saugojimo laikotarpio pažymėtina, kad, siekdami pagal šį scenarijų užtikrinti derėjimą su BDAR 5 straipsnio 1 dalies e punktu, duomenų valdytojai turėtų sugebėti pagrįsti, kodėl šio saugojimo laikotarpio šiuo tikslu reikia konkrečiais atvejais. Valdyba rekomenduoja, kad duomenų valdytojai numatytų kuo trumpesnį saugojimo laikotarpį, taip pat atsižvelgdami į tik labai retai skrendančius keleivius, ir pasiūlytų duomenų subjektams nusistatyti pageidaujamą saugojimo laikotarpį.

59. Atsižvelgdama į šiuos aspektus, atsakydama į 2.1.1 klausimą Valdyba daro išvadą, kad šis duomenų tvarkymas **iš esmės galėtų būti laikomas suderinamu su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais, jei būtų taikomos tinkamos apsaugos priemonės**.

Tinkamos apsaugos priemonės

[90] Prancūzijos PI taip paaiškino, kad gali būti ir kitų galimybių pateikti šabloną, pvz., išspausdinus popieriuje. Be to, EDAV pripažįsta, kad ateityje būtų galima numatyti naudoti alternatyvią technologiją, pvz., grindžiamą keitimosi duomenimis trumpu atstumu sistema.

[91] Taip pat būtų galima argumentuoti, kad atliekant biometrinį patikrinimą padaroma mažiau klaidų nei žmogaus atliekamo patikrinimo atveju.

60. Atsakydama į 2.1.2 klausimą, Valdyba mano, kad pagal tokį scenarijų, **be išvardytų 1 scenarijaus priemonių**, turėtų būti įgyvendinamos bent toliau nurodytos apsaugos priemonės. Siekiant įgyvendinti tuos pačius saugumo ir duomenų apsaugos tikslus, galėtų būti taikomos kitos nei šioje nuomonėje aprašytos apsaugos priemonės. Jos galėtų būti teisėtos, jei jomis užtikrinama atitiktis taikomoms teisinėms sistemoms.

61. Pastaba. *Tai bendra ir neišsami galimų tinkamų apsaugos priemonių, kurias galėtų įgyvendinti į 2 scenarijų panašų sprendimą pasirinkęs taikyti duomenų valdytojas, apžvalga. Šių priemonių tinkamumas pagal BDAR 25 ir 32 straipsnius priklausys nuo konkretaus atvejo analizės. Visi duomenų valdytojai turės užtikrinti, kad būtų atliktas jų pačių PDAV, o konkretiems jų sprendimams gali prireikti papildomų į šią nuomonę neįtrauktų priemonių.*

D. Bendrieji aspektai

D.1. Duomenų subjektų teisės ir apsaugos priemonės, kurias gali įgyvendinti duomenų valdytojai

D.1.1. Užtikrinti, kad keleiviai galėtų valdyti visų savo duomenų saugojimo laikotarpius. Saugojimo laikotarpiai turėtų būti apriboti tuo, kas būtina konkrečiam tikslui pasiekti. Atlikus išsamią tokių veiksnių kaip tapatybės nustatymo dokumento galiojimas analizę, turėtų būti nustatomas ilgiausias laikotarpis. Duomenų subjektams turėtų būti pasiūloma nustatyti pageidaujamą saugojimo laikotarpį, kuris galėtų būti trumpesnis nei numatytasis saugojimo laikotarpis.

D.1.2. Suteikti duomenų subjektui galimybę bet kuriuo metu prašyti ištrinti naudojantis mobiliąja programėle arba skaitmenine dėkle tik jo saugomus duomenis (raktą ir (arba) slaptažodį)[92].

D.1.3. Užtikrinti, kad centrinė duomenų bazė būtų tokioje vietoje, kurioje kompetentinga priežiūros institucija galėtų vykdyti veiksmingą priežiūrą.

E. Organizaciniai aspektai

E.1. Politika ir atitiktis

E.1.1. Negalima visiškai pasikliauti centriniu serveriu. Užtikrinti, kad centrinio serverio valdymui būtų taikomos aiškiai apibrėžtos valdymo taisyklės ir šis valdymas apimtų visas centrinio serverio saugumui užtikrinti būtinas priemones[93].

F. Techniniai aspektai

[92] Pažymėtina, kad ši apsaugos priemonė taikoma tik pagal 2 scenarijų.
[93] EDAV gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išsiaiškinimo priemonių, PRIV-5, p. 17.

F.1. Prieiga

F.1.1. Tvarkyti registracijos žurnalus, kuriuose nurodyta kas turi prieigą prie asmens duomenų, ypač prie TD ir biometrinių duomenų, ir kada šia prieiga buvo pasinaudota.

F.2. Infrastruktūra ir tinklas

F.2.1. Tinkamai apsaugoti centrinę duomenų bazę, taip pat nuo prieinamumo apribojimo išpuolių.

F.2.2. Užtikrinti, kad centrinė duomenų bazė, registravimo aparatai ir atitikties nustatymo įrenginiai nebūtų prijungti prie interneto. Šių sistemų veikimas ir techninė priežiūra (pvz., atsarginių kopijų darymas, pataisos, stebėsena ir pan.) turi vykti vietoje, oro uosto patalpose.

F.3. Duomenų saugumas ir valdymas

F.3.1. Siekiant apsaugoti tarp programėlės ir centralizuoto serverio vykstančius duomenų mainus, įdiegti pažangiausius kriptografijos metodus[94].

F.3.2. Individualų raktą ir (arba) slaptažodį saugoti tuo lygmeniu, kuriuo jis bus naudojamas iššifruoti (t. y. kontrolės aparate), o atitinkančiam užregistruotam biometriniam šablonui centrinėje duomenų bazėje atkurti naudoti tik indeksą.

F.3.3. Užtikrinti, kad rakto ir (arba) slaptažodžio mainais tarp naudotojo prietaiso ir kontrolės aparato ryšys būtų apsaugomas nuo bet kokio galimo neteisėto perėmimo arba perdavimo trečiosioms šalims.

F.3.4. Centrinėje duomenų bazėje saugomą biometrinį šabloną indeksuoti, kad būtų galima patvirtinti tapatybę „1 su 1“ ir užtikrinti, kad jis būtų unikalus ir susijęs su asmeniu. Užtikrinti, kad indeksas neatskleistų jokios keleivio TD informacijos ir nebūtų susietas su šifravimo raktu.

F.3.5. Tinkamai nustatyti tapatybę ir užšifruoti bet kokius tarp centrinės duomenų bazės ir kontrolės punktų perduodamus duomenis ir laikyti juos izoliuotuose tinkluose.

F.3.6. Vengti dvikrypčių ryšių tarp duomenų rinkinių (TD, biometrinių duomenų, taip pat skrydžio informacijos), o duomenų bazėje saugoti tik reikiamus vienkrypčius ryšius, pvz., tik vienkrypčius ryšius nuo indekso iki TD, nuo indekso iki šifruotų biometrinių duomenų ir nuo indekso iki skrydžio informacijos.

[94] EDAV gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išsiaiškinimo priemonių, SEC-4, p. 16: „Gali būti naudojami šie metodai: simetrinis ir asimetrinis šifravimas, maišos funkcijos, konfidencialus aibės elementų tyrimas, konfidencialus rinkinių palyginimas, „Bloom“ filtrai, konfidencialus informacijos išrinkimas, homomorfinis šifravimas“.

F.3.7. Užtikrinti veiklos tęstinumo sąlygas, pvz., taikant tinkamas atsargines saugojimo sistemas.

F.3.8. Užtikrinti, kad kontrolės aparate nebūtų saugoma šifruotų arba nešifruotų šablonų įrašų.

3.2.3 Centralizuotas užregistruotų biometrinių šablonų saugojimas tapatybei nustatyti

62. Šiame skirsnyje nagrinėjamas centralizuoto užregistruotų keleivių biometrinių šablonų saugojimo šifruota forma tapatybei nustatyti, kai šie šablonai nėra užšifruoti tik keleivių turimais raktais ir (arba) slaptažodžiais, suderinamumas su BDAR 5 straipsnio 1 dalies e bei f punktais ir 25 bei 32 straipsniais šiais dviem atvejais: 1) kai šie šablonai saugomi oro uoste esančioje duomenų bazėje oro uosto operatoriaus žinioje[95] (toliau – **3.1 scenarijus**) ir 2) kai šie šablonai saugomi debesijoje oro transporto bendrovės žinioje[96] (toliau – **3.2 scenarijus**).

63. Valdyba mano, kad, naudojant biometrinius duomenis **tapatybės nustatymo** tikslais didelėse centrinėse duomenų bazėse, suvaržomos pagrindinės duomenų subjektų teisės ir gali kilti rimtų pasekmių duomenų subjektams[97]. Be to, biometrinių duomenų naudojimą taip pat reikėtų išnagrinėti atsižvelgiant į jų tvarkymo tikslą, vadovaujantis būtinumo ir proporcingumo principais[98].

3.2.3.1 3.1 scenarijus. Centralizuotas saugojimas oro uoste esančioje duomenų bazėje oro uosto operatoriaus žinioje

Scenarijaus aprašas

64. Pagal 3.1 scenarijų užregistruoti keleivių biometriniai šablonai šifruota forma saugomi oro uosto patalpose esančioje centrinėje duomenų bazėje oro uosto operatoriaus žinioje. Pirmiausia pažymėtina, kad keleivių duomenys yra suskirstyti, t. y. jų tapatybės duomenys, užregistruoti biometriniai šablonai ir skrydžių informacija saugomi trijose skirtingose duomenų bazėse. Šie duomenys užšifruojami skirtingais raktais tiek saugojimo metu, tiek juos perduodant į atitikties nustatymo serverius, kuriuose juos paskui iššifruoja oro uosto operatorius.

65. Keleiviai turi užsiregistruoti kiekvienam skrydžiui, likus nedaug laiko iki išvykimo (pvz., prieš 48 valandas). Ši registracija gali būti atliekama nuotoliniu būdu arba oro uosto terminaluose, laikantis tinkamo tapatybės saugumo užtikrinimo lygio (pvz., tinkamo sistemos *eIDAS* saugumo užtikrinimo lygio). Registracija taip pat gali vykti taip, kaip aprašyta pagal 1 scenarijų – šiuo atveju keleiviai per 48 valandų laikotarpį iki išvykimo turi perduoti savo duomenis iš savo skaitmeninių dėklių į oro uosto sistemą.

---

[95] Remiantis Prašymo I priede pateiktu 3A naudojimo atvejo pavyzdžiu.
[96] Remiantis Prašymo I priede pateiktu 3B naudojimo atvejo pavyzdžiu.
[97] Pavyzdžiui, žr. 29 straipsnio darbo grupės nuomonę 3/2012 dėl biometrinių technologijų, p. 8. Taip pat žr. pirmiau išdėstytą 26 punktą.
[98] BDAR 4 konstatuojamoji dalis. Taip pat žr. 29 straipsnio darbo grupės nuomonę 3/2012 dėl biometrinių technologijų, p. 8.

66. Pagal šį scenarijų keleiviai taip pat atvyksta prie specialaus kontrolės aparato, kuriame įrengta kamera. Tada jų biometrinių duomenų pavyzdys išsiunčiamas į centrinį oro uosto serverį, kuriame stengiamasi nustatyti, ar šie duomenys sutampa su centrinėje biometrinių duomenų bazėje saugomais duomenimis. Taip galima nustatyti keleivių tapatybę ir patikrinti, ar jie iš tikrųjų yra užsiregistravę skrydžiui (arba įlaipinimui, jei kontrolė atliekama įlaipinant). Atsižvelgiant į kontrolės punktą, užklausą pateikusiam kontrolės punkte dirbančiam duomenų valdytojui atgal siunčiamų duomenų kiekis gali būti sumažinamas, pvz., pateikiant atsakymą „Taip“ / „Ne“ arba, jei reikia, patį atitikties nustatymo rezultatą. Šiuo atveju kontrolės punkte dirbančiam duomenų valdytojui perduodamas tik užklausos rezultatas ir šis duomenų valdytojas naudoja tik jį.

67. Konkrečiai pažymėtina, kad pagal šį scenarijų yra nustatoma keleivių tapatybė (atliekamas palyginimas „1 su N“, kai N yra per kelių dienų laikotarpį oro uoste laukiamas keleivių skaičius). Be to, biometrinių duomenų atitiktis nustatoma tik kiekvienam keleiviui atvykus prie iš anksto nustatyto išvykimo oro uosto kontrolės punkto, bet duomenų tvarkymas atliekamas centriniame serveryje, kuris yra prijungtas prie centrinės duomenų bazės. Pagal šį scenarijų saugojimo laikotarpis paprastai yra 48 valandos, o duomenys ištrinami, kai tik lėktuvas pakyla.

EDAV vertinimas

68. Kaip priminta pirmiau, tvarkant biometrinius duomenis, kyla didesni pavojai duomenų subjektų teisėms ir laisvėms[99]. Todėl bet koks duomenų saugumo pažeidimas gali turėti itin rimtų pasekmių duomenų subjektams[100]. Duomenų valdytojai privalo šiuos pavojus veiksmingai mažinti. Kadangi pagal šį scenarijų visa struktūra yra visiškai centralizuota, keleiviai labiau praranda savo duomenų kontrolę. Be to, taip pat galėtų kilti didesnis pavojus, kad duomenys galiausiai bus tvarkomi kitais nei keleivių srauto valdymo tikslais.

69. Atsižvelgiant į saugumo principą ir reikalavimus (BDAR 5 straipsnio 1 dalies f punktas ir 32 straipsnis), reikėtų atsižvelgti į tai, kad saugant TD ir biometrinius duomenis centrinėse duomenų bazėse, nors jos ir atskirtos,, gali atsirasti didelių paskatų išpuoliams, o pažeidus šių duomenų bazių konfidencialumą galima įgyti prieigą prie viso duomenų rinkinio. Todėl galimas su veido atpažinimo šablonais ir susijusiais TD susijęs pažeidimas gali sudaryti sąlygas neleistinai arba neteisėtai nustatyti duomenų subjektų tapatybę kitose aplinkose. Atsižvelgiant į biometriniam tapatybės nustatymui taikomus metodus, taip pat gali kilti grėsmė tolesniam saugiam veido atpažinimo šablonų, kaip identifikatorių, naudojimui. Šiuo atveju, kitaip nei naudojant kitos rūšies kredencialus (pvz., naudotojo identifikatorių, slaptažodį), kuriuos galima pakeisti, pažeidimo poveikio sumažinti neįmanoma[101].

70. Be to, kadangi duomenų valdytojas turi labai daug kokybiškų TD ir biometrinių duomenų, išpuolių rengėjams jie tampa labai patraukliu taikiniu, todėl dėl pavojaus saugumui tai kelia didesnę tikimybę. Be to, duomenų pažeidimų poveikis galėtų būti didesnis, nes duomenys saugomi centralizuotoje vietoje, todėl išpuolių rengėjams galėtų būti lengviau įgyti prieigą prie asmens duomenų, kurie yra susiję su daugeliu keleivių. Taigi, galimas pažeidimas dideliam skaičiui duomenų subjektų galėtų sukelti

[99] Žr. pirmiau išdėstytą 26 punktą.
[100] Gairės dėl veido atpažinimo, Europos Tarybos konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu patariamasis komitetas, 2021 m. birželio mėn., p. 22,
[101] Šiuo atžvilgiu žr. 29 straipsnio darbo grupės nuomonę 3/2012 dėl biometrinių technologijų, p. 34.

sunkumo atžvilgiu didelių, pvz., plataus masto tapatybės vagystės, pavojų, kuriuos itin sunku sumažinti.

71. Todėl suderinamumo su BDAR 5 straipsnio 1 dalies f punktu ir 32 straipsniu atžvilgiu pažymėtina, kad, atsižvelgiant į techninių galimybių išsivystymo lygį, pagal 3.1 scenarijų numatytų priemonių[102], nepakanka, kad būtų užtikrintas pavojų atitinkančio lygio saugumas. Tuo remiantis pažymėtina, kad, jei duomenų valdytojas apsiribotų tik šiomis priemonėmis, duomenų tvarkymas pagal 3.1 scenarijų neatitiktų BDAR 5 straipsnio 1 dalies f punkto ir 32 straipsnio.

72. Dėl BDAR 5 straipsnio 1 dalies e punkte nustatyto principo pažymėtina, kad pagal šį scenarijų biometrinių duomenų saugojimo centrinėje duomenų bazėje laikotarpis paprastai yra 48 valandos. Atrodo, kad tokiu saugojimo laikotarpio apribojimu labai sumažinami su asmens duomenų pažeidimais susiję pavojai. Vis dėlto duomenų saugojimo laikotarpis savaime nėra esminis bendrojo nurodytos struktūros suderinamumo veiksnys, nes tokius duomenų laikymo laikotarpius duomenų valdytojai gali keisti. Siūlomos priemonės bet kuriuo atveju turi atitikti BDAR 25 straipsnyje nustatytus pritaikytosios ir standartizuotosios duomenų apsaugos reikalavimus.

73. Kitaip nei pagal 1 ir 2 scenarijus, kai keleivių tapatybė yra patvirtinama, pagal 3.1 scenarijų keleivių tapatybė yra nustatoma (atliekamas palyginimas „1 su N“, kai N yra per kelių dienų laikotarpį oro uoste laukiamas dėl šio tvarkymo einant per specialius oro uosto kontrolės punktus sutikimą davusių keleivių skaičius). Šiuo tikslu keleivių ieškoma centrinėje duomenų bazėje ir tvarkomas kiekvienas užregistruotas biometrinių duomenų pavyzdys, siekiant patikrinti, ar jis atitinka sistemoje žinomą asmenį. Pagal 3.1 scenarijų, kitaip nei pagal 2 scenarijų, raktus turi ne tik keleiviai. Taigi, pagal šį scenarijų keleiviai gali daug mažiau kontroliuoti savo biometrinius duomenis. Todėl šis pagal 3.1 scenarijų siūlomas duomenų tvarkymas negali būti suderinamas su BDAR 25 straipsnyje nustatytais pritaikytosios duomenų apsaugos ir projektavimo reikalavimais.

74. Laikydamiesi BDAR 25 straipsnio duomenų valdytojai turėtų atsižvelgti į duomenų tvarkymo tikslais būtinų asmens duomenų rūšis, kategorijas ir išsamumo lygį[103]. Rinkdamiesi projektavimo sprendimus jie turėtų atsižvelgti į renkant didelį išsamių asmens duomenų kiekį kylančius didesnius pavojus duomenų kiekio mažinimo, vientisumo, konfidencialumo bei saugojimo trukmės apribojimo principams ir palyginti juos su mažesniais pavojais renkant mažesnį kiekį ir (arba) mažiau išsamią informaciją apie duomenų subjektus. Bet kuriuo atveju pagal numatytąsias nuostatas neturėtų būti renkami asmens duomenys, kurie nėra būtini konkrečiu duomenų tvarkymo tikslu. Kitaip tariant, jei tam tikrų kategorijų asmens duomenys yra nebūtini arba nereikia išsamių duomenų, nes pakanka mažiau detalių duomenų, jokie pertekliniai asmens duomenys neturėtų būti renkami. Jei šiuo atveju tą patį tikslą būtų galima pasiekti įgyvendinant kitokį duomenų tvarkymą ir pagal 3.1 scenarijų aprašytomis sąlygomis, veido atpažinimo technologijos naudoti nebūtina.

75. Dėl BDAR 25 straipsnio pažymėtina, kad vienas iš pagrindinių pritaikytosios ir standartizuotosios duomenų apsaugos elementų yra duomenų subjekto savarankiškumas. Konkrečiai duomenų subjektams turėtų būti suteikta kuo daugiau savarankiškumo priimant sprendimus dėl jų asmens duomenų naudojimo, taip pat dėl to duomenų naudojimo arba tvarkymo apimties ir sąlygų[104]. Pagal 1

[102] Kaip aprašyta pirmiau 64–67 punktuose.

[103] EDAV gairių 4/2019 dėl pritaikytosios ir standartizuotosios duomenų apsaugos 49 punktas.

[104] EDAV gairių 4/2019 dėl pritaikytosios ir standartizuotosios duomenų apsaugos 70 punktas. BDAR 7 konstatuojamojoje dalyje taip pat paaiškinta, kad „[f]iziniai asmenys turėtų kontroliuoti savo asmens duomenis“.

scenarijų duomenų subjektas turėtų su jo biometrinio šablono naudojimu, atskleidimu ir ištrynimu susijusį savarankiškumą ir kontrolę, o pagal 2 scenarijų išlaikytų kai kurią su jo biometrinio šablono atskleidimu susijusią kontrolę, nes šifravimo raktą ir (arba) slaptažodį saugotų pas save. Tačiau pagal 3.1 scenarijų duomenų subjektas visiškai priklauso nuo to, kaip jo biometrinius duomenis nusprendžia tvarkyti duomenų valdytojas, todėl negali kontroliuoti savo biometrinio šablono naudojimo tiesiogiai.

76. Atsižvelgiant į BDAR 25 straipsnį, ypač siekiant laikytis duomenų kiekio mažinimo reikalavimo, pagal 3.1 scenarijų numatytas duomenų tvarkymas negali atitikti būtinumo principo. Valdyba mano, kad panašų keleivių srautų racionalizavimo oro uostuose rezultatą galima pasiekti privatumą varžant mažiau. Pavyzdžiui, jį galima pasiekti nenaudojant biometrinių duomenų (nors tada naudotojų patirtis būtų kitokia, nes jų įlaipinimo talonų ir prireikus oficialių tapatybės nustatymo dokumentų patikrinimas gali užtrukti ilgiau). Be to, tikslus galima pasiekti mažiau suvaržant privatumą, pasirinkus kitus sprendimus, ypač tokius, kurie grindžiami biometrinių duomenų saugojimu vietos dėklėje asmens prietaise arba kuriuos taikant reikalaujama užšifruoti duomenis specialiu asmens prietaise saugomu raktu.

77. Dėl proporcingumo principo pažymėtina, kad pagal 3.1 scenarijų numatytas duomenų tvarkymas keltų tokius pavojus duomenų subjektų teisėms, kurie, atsižvelgiant į techninių galimybių išsivystymo lygį, nebūtų sumažinti numatytomis priemonėmis. Atrodo, kad neigiamo poveikio duomenų subjektų teisėms ir laisvėms pavojus, kuris galėtų atsirasti dėl duomenų pažeidimo centralizuotoje didelio skaičiaus asmenų biometrinių duomenų bazėje, nusveria numatomą duomenų tvarkymo naudą, nes ši nauda yra palyginti nedidelė, t. y. tik šiek tiek didesnis patogumas ir spartesni patikrinimai. Todėl ja negalima pagrįsti didelio varžomojo šių priemonių poveikio pagrindinėms asmenų teisėms bei laisvėms, o pagal 3.1 scenarijų numatytas duomenų tvarkymas neatitinka proporcingumo principo.

78. Atsižvelgdama į šiuos pasvarstymus Valdyba, atsakydama į 2.2.1 klausimą, daro išvadą, kad, kai duomenys tvarkomi siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose, pagal 3.1 scenarijų numatytas duomenų tvarkymas:

    - **negali būti suderinamas su BDAR 25 straipsniu**;
    - jei duomenų valdytojas apsiribotų tik pagal 3.1 scenarijų aprašytomis priemonėmis, **nesilaikytų BDAR 5 straipsnio 1 dalies f punkto ir 32 straipsnio**.

3.2.3.2 3.2 scenarijus. Centralizuotas saugojimas debesijoje oro transporto bendrovės žinioje

Scenarijaus aprašas

79. Pagal 3.2 scenarijų užregistruoti keleivių biometriniai šablonai saugomi debesijoje oro transporto bendrovės arba jos debesijos paslaugų teikėjo (duomenų tvarkytojo) žinioje. Prašyme nurodyta, kad debesijos paslaugų teikėjas būtų įsisteigęs EEE[105]. Šiuo atveju keleivių duomenys yra užšifruojami, bet naudojimo metu (pvz., atliekant atitikties nustatymo operaciją) yra iššifruojami, o raktus valdo oro transporto bendrovė arba jos debesijos duomenų tvarkytojas. Keleivių biometriniai duomenys naudojami keleivių tapatybei nustatyti (palyginimas „1 su N“, kai N gali būti visas oro transporto bendrovės klientų skaičius)[106].

80. Pagal šį scenarijų, panašiai kaip pagal 1, 2 ir 3.1 scenarijus, keleiviai taip pat pirmiausia turi užsiregistruoti. Tačiau pagal 3.2 scenarijų keleivių registracija atliekama vieną kartą ir galioja tol, kol klientas turi paskyrą toje oro transporto bendrovėje. Registracija atliekama nuotoliniu būdu, laikantis tinkamo tapatybės saugumo užtikrinimo lygio (pvz., tinkamo sistemos *eIDAS* saugumo užtikrinimo lygio), arba oro uostų terminaluose. Biometrinių duomenų atitiktis nustatoma tik keleiviams atvykus prie iš anksto nustatytų oro uosto kontrolės punktų, bet duomenų tvarkymas atliekamas debesijoje.

81. Oro uoste keleiviai eina pro specialius kontrolės aparatus, kuriose įrengtos kameros. Keleivių biometriniai duomenys siunčiami pateikiant užklausą oro transporto bendrovės debesijos serveriui, kuriame tikrinama, ar šie duomenys sutampa su centrinėje duomenų bazėje esančiais duomenimis. Taip galima nustatyti keleivių tapatybę ir patikrinti, ar jie iš tikrųjų yra užsiregistravę skrydžiui (arba įlaipinimui, jei kontrolė atliekama įlaipinant).

82. Atitikties nustatymo rezultatai galėtų būti pateikiami keliems oro uostų operatoriams, jei oro transporto bendrovė turi specialų terminalą arba prieigą prie bendros oro uosto informacinės sistemos infrastruktūros. Atsižvelgiant į kontrolės punktą, užklausą pateikusiam kontrolės punkte dirbančiam duomenų valdytojui atgal siunčiamų duomenų kiekis gali būti sumažinamas, pvz., pateikiant atsakymą „Taip“ / „Ne“ arba, jei reikia, patį atitikties nustatymo rezultatą. Šiuo atveju patikrinimą kontrolės punkte atliekantis duomenų valdytojas sužino ir naudoja tik užklausos rezultatą.

83. Šablono saugojimo laikotarpį nustato oro transporto bendrovė. Jis galėtų trukti tol, kol klientas turi paskyrą toje oro transporto bendrovėje.

EDAV vertinimas

84. Su 3.1 scenarijumi susiję Valdybos jau išdėstyti aspektai[107] taikomi ir šiam scenarijui.

85. Dėl saugumo principo ir reikalavimų (BDAR 5 straipsnio 1 dalies f punktas ir 32 straipsnis) pažymėtina, kad pagal 3.2 scenarijų duomenų tvarkymas atliekamas debesijoje ir prieigą prie šių duomenų galėtų

[105] Prancūzijos PI paaiškino, kad tai tėra pavyzdys ir kad taip pat būtų galima įtraukti debesijos paslaugų teikėjus, kurie yra įsisteigę ne EEE. Be to, taip pat būtų galima numatyti kitus saugojimo sprendimus (pvz., nesinaudojant debesija).
[106] Prancūzijos PI paaiškino, kad tai tėra pavyzdys ir kad esama sprendimų, pagal kuriuos biometriniai duomenys perduodami kaskart prieš skrydį.
[107] Pirmiau išdėstyti 68–77 punktai.

turėti keli subjektai, taip pat galbūt ne EEE paslaugų teikėjai, net jei duomenys laikomi EEE[108]. Šiai struktūrai būdingi galimi pavojai, susiję su asmens duomenų perdavimu į trečiąsias valstybes. Be to, nors keleivių duomenys yra užšifruojami, naudojimo metu (t. y. vykdant atitikties nustatymo operaciją) jie yra iššifruojami, o raktus kontroliuoja oro transporto bendrovė arba jos debesijos duomenų tvarkytojas. Taip juos saugant, gali dar labiau padidėti pavojų saugumui perimetras.

86. Todėl dėl suderinamumo su BDAR 5 straipsnio 1 dalies f punktu ir 32 straipsniu pažymėtina, kad, atsižvelgiant į techninių galimybių išsivystymo lygį, pagal 3.2 scenarijų numatytų priemonių[109] nepakanka, kad būtų užtikrintas pavojų atitinkančio lygio saugumas. Tuo remiantis pažymėtina, kad, jei duomenų valdytojai apsiribotų tik šiomis priemonėmis, duomenų tvarkymas pagal 3.2 scenarijų neatitiktų BDAR 5 straipsnio 1 dalies f punkto ir 32 straipsnio.

87. Be to, pagal 3.2 scenarijų[110] duomenys galėtų būti saugomi labai ilgą laikotarpį (t. y. galbūt tol, kol duomenų subjektas turi paskyrą toje oro transporto bendrovėje). Ši saugojimo trukmė kelia didesnius duomenų konfidencialumo ir vientisumo pažeidimo pavojus ir, atrodo, viršija tai, kas tikrai būtina ir proporcinga duomenų tvarkymo tikslais. Valdyba atkreipia dėmesį į tai, kad duomenų saugojimo laikotarpis savaime nėra esminis bendrojo nurodytos struktūros suderinamumo su BDAR veiksnys, nes duomenų valdytojai jį gali keisti. Vis dėlto, atsižvelgiant į Valdybos turimą ir 3.2 scenarijaus apraše pateiktą informaciją, šis ilgas saugojimo laikotarpis nėra pakankamai pagrįstas ir nėra akivaizdžių priemonių, kuriomis būtų galima sumažinti asmenims kylančius pavojus. Tuo remiantis, siūlomas saugojimo laikotarpis nebūtų apribotas tuo, kas būtina, kaip reikalaujama pagal BDAR 5 straipsnio 1 dalies e punkte nustatytą saugojimo trukmės apribojimo principą.

88. Bet kuriuo atveju pagal 3.2 scenarijų siūlomos priemonės negali atitikti BDAR 25 straipsnyje nustatytų pritaikytosios duomenų apsaugos ir projektavimo reikalavimų. Pagal 3.2 scenarijų užregistruoti keleivių biometriniai šablonai saugomi debesijoje oro transporto bendrovės arba jos debesijos paslaugų teikėjo (duomenų tvarkytojo) žinioje. Kaip aprašyta pirmiau, prieigą prie šių duomenų galbūt galėtų turėti keli subjektai. Be to, keleivių biometriniai duomenys naudojami keleivių tapatybei nustatyti (palyginimas „1 su N“, kai N gali būti visas naudotojų ir (arba) oro transporto bendrovės klientų skaičius). Pagal šį metodą centrinėje duomenų bazėje asmenų grupėje ieškoma asmens, tvarkant kiekvieno užfiksuoto veido duomenis, siekiant patikrinti, ar jie sutampa su sistemoje žinomo asmens duomenimis. Pagal 3.2 scenarijų, kitaip nei pagal 3.1 scenarijų, palyginimas gali būti atliekamas daug platesniu mastu, nes šiuo atveju kriterijus yra visų oro transporto bendrovės klientų skaičius, o ne, kaip pagal 3.1 scenarijų, tik per kelių dienų laikotarpį laukiamas keleivių skaičius.

89. Be to, atsižvelgiant į BDAR 25 straipsnį, ypač siekiant laikytis duomenų kiekio mažinimo reikalavimo, pagal 3.2 scenarijų numatytas duomenų tvarkymas negali atitikti būtinumo principo. Valdyba mano, kad panašų keleivių srautų racionalizavimo oro uostuose rezultatą būtų galima pasiekti kitomis mažiau varžančiomis priemonėmis, pvz., nenaudojant biometrinių duomenų, nors tada naudotojų patirtis skirtųsi, nes jų tapatybės nustatymo dokumentų ir įlaipinimo talonų patikrinimas gali ilgiau užtrukti. Be to, duomenų valdytojas tikslus gali pasiekti mažiau suvaržydamas privatumą, pasirinkdamas kitus

[108] 2023 m. sausio 17 d. EDAV dokumentas *2022 Coordinated Enforcement Action on the use of cloud-based services by the public sector* (liet. „2022 m. koordinuoti vykdymo užtikrinimo veiksmai dėl viešojo sektoriaus naudojimosi debesija grindžiamomis paslaugomis“), p. 19.
[109] Žr. pirmiau išdėstytus 79–83 punktus.
[110] Žr. pirmiau išdėstytą 83 punktą.

sprendimus, ypač tokius, kurie grindžiami biometrinių duomenų saugojimu vietos dėklėje asmeniniame prietaise arba pagal kuriuos reikalaujama užšifruoti duomenis specialiu asmeniame prietaise saugomu raktu.

90. Dėl proporcingumo principo pažymėtina, kad pagal 3.2 scenarijų numatytas duomenų tvarkymas keltų pavojus duomenų subjektų teisėms, kurie nebūtų sumažinami numatytomis apsaugos priemonėmis. Atrodo, kad neigiamas poveikis duomenų subjektų teisėms ir laisvėms, kuris atsirastų dėl duomenų pažeidimo debesijoje saugomoje centralizuotoje didelio skaičiaus asmenų biometrinių duomenų bazėje, nusveria numatomą duomenų tvarkymo naudą, nes ši nauda yra palyginti nedidelė, t. y. tik šiek tiek didesnis patogumas ir spartesni patikrinimai. Todėl ja negalima pagrįsti didelio varžomojo šių priemonių poveikio pagrindinėms asmenų teisėms ir laisvėms ir pagal 3.2 scenarijų numatytas duomenų tvarkymas negali būti laikomas proporcingu.

91. Atsižvelgdama į šiuos aspektus Valdyba, atsakydama į 2.3.1 klausimą, daro išvadą, kad, kai duomenų tvarkymas atliekamas siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose, pagal 3.2 scenarijų numatytas duomenų tvarkymas:

- **negali būti suderinamas su BDAR 25 straipsniu**,
- **neatitiktų BDAR 5 straipsnio 1 dalies f punkto ir 32 straipsnio**, jei duomenų valdytojai apsiribotų tik pagal 3.2 scenarijų aprašytomis priemonėmis, ir,
- **neatitiktų BDAR 5 straipsnio 1 dalies e punkto**, nes, remiantis Valdybos turima informacija, pagal 3.2 scenarijų numatytas laikymo laikotarpis nėra pakankamai pagrįstas. Norėdamas laikytis BDAR 5 straipsnio 1 dalies e punkte nustatyto saugojimo trukmės apribojimo principo, duomenų valdytojas turėtų įrodyti, kad asmens duomenys yra saugomi ne ilgiau, nei būtina jų tvarkymo tikslais.

4 IŠVADOS

92. 1.1 klausimu dėl BDAR 5 straipsnio 1 dalies f punkto ir 25 bei 32 straipsnių, remdamasi Prancūzijos PI prašymu pateikti nuomonę ir pirmiau pateikta analize, Valdyba daro šią išvadą:

93. veido atpažinimo technologijos naudojimas biometriniam tapatybės patvirtinimui, siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose (saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose), iš esmės galėtų būti laikomas suderinamu su BDAR 5 straipsnio 1 dalies f punkte ir 25 bei 32 straipsniuose nustatytais vientisumo ir konfidencialumo principais, taikant saugojimo struktūrą, kai užregistruotas kiekvieno keleivio biometrinis šablonas saugomas vietoje tik jo kontroliuojamame asmeniniame prietaise, jei būtų taikomos tinkamos nuo pirmiau išdėstyto 46 punkto aprašomos apsaugos priemonės.

94. 2.1.1 klausimu dėl BDAR 5 straipsnio 1 dalies e bei f punktų ir 25 bei 32 straipsnių, remdamasi Prancūzijos PI prašymu pateikti nuomonę ir pirmiau pateikta analize, Valdyba daro šią išvadą:

95. veido atpažinimo technologijos naudojimas biometriniam tapatybės patvirtinimui, siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose (saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose), iš esmės galėtų būti laikomas suderinamu su BDAR 5 straipsnio 1 dalies e punkte nustatytu saugojimo trukmės apribojimo principu ir 5 straipsnio 1 dalies f punkte ir 25 bei 32 straipsniuose nustatytais vientisumo ir konfidencialumo principais, taikant tokią centralizuoto saugojimo struktūrą, kai užregistruotas kiekvieno keleivio biometrinis šablonas šifruota forma saugomas oro uoste centrinėje duomenų bazėje oro uosto operatoriaus žinioje, o

raktą ir (arba) slaptažodį turi tik asmuo, jei būtų taikomos tinkamos nuo pirmiau išdėstyto 60 punkto aprašomos apsaugos priemonės.

96. 2.2.1 klausimu dėl BDAR 5 straipsnio 1 dalies e bei f punktų ir 25 bei 32 straipsnių, remdamasi Prancūzijos PI prašymu pateikti nuomonę ir pirmiau pateikta analize, Valdyba daro šią išvadą:

97. veido atpažinimo technologijos naudojimas biometriniam tapatybės nustatymui, siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose (saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose), kai taikoma tokia centralizuoto saugojimo struktūra, kai užregistruoti keleivių biometriniai šablonai nėra užšifruoti tik kiekvieno keleivio turimu raktu ir (arba) slaptažodžiu, šie šablonai saugomi oro uoste (oro uosto operatoriaus žinioje) duomenų bazėje, negali būti suderinamas su BDAR 25 straipsniu. Be to, jei duomenų valdytojai apsiribotų tik pagal 3.1 scenarijų aprašytomis priemonėmis, šis duomenų tvarkymas neatitiktų BDAR 5 straipsnio 1 dalies f punkte ir 32 straipsnyje nustatytų vientisumo ir konfidencialumo principų.

98. 2.3.1 klausimu dėl BDAR 5 straipsnio 1 dalies e bei f punktų ir 25 bei 32 straipsnių, remdamasi Prancūzijos PI prašymu pateikti nuomonę ir pirmiau pateikta analize, Valdyba daro šią išvadą:

99. veido atpažinimo technologijos naudojimas biometriniam tapatybės nustatymui, siekiant konkrečiai racionalizuoti keleivių srautus oro uostuose (saugumo kontrolės punktuose, bagažo pridavimo, įlaipinimo ir patekimo į keleivių laukiamuosius vietose), kai taikoma tokia centralizuoto saugojimo struktūra, kai užregistruoti keleivių biometriniai šablonai nėra užšifruoti tik kiekvieno keleivio turimu raktu ir (arba) slaptažodžiu, šie šablonai saugomi (oro transporto bendrovės žinioje esančioje) debesijoje, negali būti suderinamas su BDAR 25 straipsniu. Be to, jei duomenų valdytojai apsiribotų tik pagal 3.2 scenarijų aprašytomis priemonėmis, šis duomenų tvarkymas neatitiktų BDAR 5 straipsnio 1 dalies f punkte ir 32 straipsnyje nustatytų vientisumo ir konfidencialumo principų. Galiausiai, remiantis 3.2 scenarijaus aprašu ir Valdybos turima informacija, šis duomenų tvarkymas neatitiktų BDAR 5 straipsnio 1 dalies e punkte nustatyto saugojimo trukmės apribojimo principo.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Anu Talus)