Andmekaitsenõukogu arvamus (art 64)

Arvamus 11/2024, mis käsitleb näotuvastustehnoloogiate kasutamist lennujaama reisijatevoo sujuvamaks muutmisel (kooskõlas IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32)

Versioon 1.1

Vastu võetud 23. mail 2024

Versioon 1.1	28. mai 2024	Grammatiline parandus kommenteeritud kokkuvõttes (lk 3 ja 4) ning arvamuse punktid 77 ja 90
Versioon 1.0	23. mai 2024	Arvamuse vastuvõtmine

Kokkuvõte

Prantsusmaa järelevalveasutus palus Euroopa Andmekaitsenõukogul esitada arvamus näotuvastustehnoloogia kasutamise kohta lennujaamade käitajate ja lennufirmade poolt reisijate biomeetrilise autentimise või tuvastamise eesmärgil, et muuta lennujaamades reisijatevood sujuvamaks.

Sissejuhatava märkusena tuletab andmekaitsenõukogu meelde, et biomeetriliste andmete ja eelkõige näotuvastustehnoloogia kasutamine kujutab endast kõrgemat ohtu andmesubjektide õigustele ja vabadustele. See puudutab biomeetriliste andmete töötlemist. Biomeetrilised andmed on isikuandmete kaitse üldmääruse artikli 9 alusel erilise kaitse all. Enne selliste tehnoloogiate kasutamist, isegi kui neid peetakse eriti tõhusaks, peaksid vastutavad töötlejad hindama nende mõju andmesubjektide põhiõigustele ja -vabadustele ning kaaluma, kas töötlemise õiguspärast eesmärki saaks saavutada vähem sekkuvate vahenditega.

Käesolevas arvamuses käsitletakse vastavalt taotlusele ainult seda, kuivõrd on töötlemine kooskõlas **isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32**, pidades silmas **eesmärki muuta lennujaamade reisijatevoog sujuvamaks** neljas konkreetses kontrollpunktis, nimelt julgestuskontrollis, pagasi äraandmisel, pardaleminekul ja reisijate juurdepääsul *lounge*'ile. Käesolev arvamus ei sisalda täielikku analüüsi selle kohta, kas asjaomane(asjaomased) vastutav(ad) töötleja(d) ja vajaduse korral nende volitatud töötleja(d) järgivad isikuandmete kaitse üldmäärust. Seetõttu ei piira käesolev arvamus vastutava töötleja konkreetsel kavandataval töötlemistoimingul ja asjaoludel põhinevat juhtumipõhist õiguslikku ja tehnilist analüüsi. Lisaks ei hõlma andmekaitsenõukogule taotluses esitatud küsimused kohaldatava õigusliku aluse analüüsi ja seetõttu ei analüüsita käesolevas arvamuses selliseks töötlemiseks antud nõusoleku kehtivust kooskõlas isikuandmete kaitse üldmääruse artiklitega 6, 7 ja 9. Lisaks ei piira käesolev ettepanek liikmesriikide õiguses sätestatud biomeetriliste andmete kasutamise piirangute kohaldamist.

Käesolevas arvamuses hindab andmekaitsenõukogu isikuandmete töötlemise vastavust eespool nimetatud isikuandmete kaitse üldmääruse sätetele **nelja konkreetse stsenaariumi** kontekstis.

Esimene stsenaarium hõlmab registreeritud biomeetrilise malli säilitamist üksikisiku valduses, näiteks tema individuaalses seadmes, tema ainukontrolli all, et autentida (1:1 võrdlus) reisija eespool nimetatud lennujaama kontrollpunktide läbimisel.

Andmekaitsenõukogu järeldab, et valitud meetmeid võib pidada vajalikkuse põhimõttele vastavaks, kui vastutav töötleja suudab tõendada, et puuduvad vähem sekkuvad alternatiivsed lahendused, mis suudaksid sama eesmärki tõhusalt saavutada. Lisaks saab töötlemise sekkuvust tasakaalustada reisijate aktiivse kaasamisega, kuna nende biomeetriline mall on nende endi valduses, näiteks nende individuaalses seadmes, nende ainukontrolli all ning nende andmed kustutatakse lühidalt pärast andmete võrdlemise lõpuleviimist. Selle põhjal järeldab andmekaitsenõukogu, et esimeses stsenaariumis kavandatud töötlemist **võib pidada põhimõtteliselt isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktiga f ning artiklitega 25 ja 32 kooskõlas olevaks**, kui rakendatakse asjakohaseid kaitsemeetmeid.

Andmekaitsenõukogu on kindlaks määranud miinimum kaitsemeetmed, mida esimese stsenaariumiga sarnase lahenduse puhul rakendada tuleks.

Teine stsenaarium hõlmab registreeritud biomeetrilise malli tsentraliseeritud säilitamist lennujaamas krüpteeritud kujul kus võti/saladus on üksnes reisija valduses. See võimaldab reisijate autentimist (1:1 võrdlus) eespool nimetatud lennujaama kontrollpunktide läbimisel. Registreering kehtib teatava ajavahemiku jooksul, mis võib näiteks olla kuni üks aasta pärast viimase lennu väljumist või kuni passi kehtivusaja lõpuni.

Andmekaitsenõukogu järeldab, et töötlemist võib pidada vajalikkuse põhimõttele vastavaks, kui vastutav töötleja suudab tõendada, et puuduvad vähem sekkuvad alternatiivid, mis suudaksid sama eesmärki tõhusalt saavutada. Lisaks saab töötlemise sekkuvust tasakaalustada reisija aktiivse kaasamisega, kuna tema krüpteeritud biomeetriliste andmete võti/saladus on tema ainukontrolli all. Eeldades, et vastutav töötleja rakendab asjakohaseid kaitsemeetmeid, saaks selle stsenaariumi korral keskse andmebaasi kasutamisest tulenevaid turvaohte leevendada ning negatiivset mõju andmesubjektide põhiõigustele ja -vabadustele võiks pidada proportsionaalseks eeldatava kasuga. Mis puudutab säilitamise piirangu põhimõtet, siis ei ole andmekaitsenõukogule esitatud teavet pika säilitamistähtaja põhjendamiseks. Selleks et saavutada selle stsenaariumi puhul kooskõla isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktiga e, peaksid vastutavad töötlejad suutma põhjendada, miks kavandatav säilitamistähtaeg on konkreetsetel juhtudel eesmärgi saavutamiseks vajalik. Andmekaitsenõukogu soovitab vastutavatel töötlejatel kehtestada võimalikult lühike säilitamistähtaeg, pakkudes samas reisijatele võimalust valida säilitamistähtaeg, mida nemad eelistavad. Selle põhjal järeldab andmekaitsenõukogu, et teises stsenaariumis kavandatud töötlemist **võib pidada põhimõtteliselt isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32 kooskõlas olevaks**, kui rakendatakse asjakohaseid kaitsemeetmeid.

Andmekaitsenõukogu on kindlaks määranud minimaalsed kaitsemeetmed, mida teise stsenaariumiga sarnase lahenduse puhul rakendada tuleks.

Kolmas stsenaarium hõlmab registreeritud biomeetrilise malli tsentraliseeritud säilitamist lennujaamas krüpteeritud kujul lennujaama käitaja kontrolli all. See võimaldab reisijate tuvastamist (1:1 võrdlus) eespool nimetatud lennujaama kontrollpunktide läbimisel. Selle stsenaariumi puhul on säilitamistähtaeg tavaliselt 48 tundi ja andmed kustutatakse pärast lennuki õhkutõusmist.

Kuna isikutuvastus andmeid ja biomeetrilisi andmeid säilitatakse keskses andmebaasis, võib andmebaasi konfidentsiaalsuse ohtu sattumisel tekkida juurdepääs kogu andmekogumile ja saada võimalikuks reisijate loata või ebaseaduslik tuvastamine muudes keskkondades. Lennujaama käitaja kontrolli all olev tsentraliseeritud säilitusarhitektuur tähendab ka seda, et reisija kontroll oma andmete üle üha väheneb. Andmekaitsenõukogu leiab, et sarnast tulemust lennujaamades reisijatevoo sujuvamaks muutmisel on võimalik saavutada vähem sekkuval viisil ning negatiivne mõju andmesubjektide põhiõigustele ja -vabadustele, mis tuleneb andmetega seotud rikkumisest biomeetriliste andmete keskandmebaasis, näib kaaluvat üles töötlemisest tuleneva eeldatava kasu. Seetõttu ei vasta töötlemine vajalikkuse ja proportsionaalsuse põhimõtetele. Selle põhjal järeldab andmekaitsenõukogu, et kolmandas stsenaariumis ette nähtud töötlemist **ei saa lugeda isikuandmete kaitse üldmääruse artikliga 25 kooskõlas olevaks**. **Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktiga f ja artikliga 32** ei oleks kooskõlas ka see, kui vastutav töötleja piirduks käesolevas stsenaariumis kirjeldatud meetmetega.

Neljas stsenaarium hõlmab registreeritud biomeetrilise malli tsentraliseeritud säilitamist pilves krüpteeritud kujul lennufirma või tema pilveteenuse osutaja kontrolli all. See võimaldab reisijate tuvastamist (1:N võrdlus) eespool nimetatud lennujaama kontrollpunktide läbimisel. Selle stsenaariumi puhul võib säilitusaeg kesta sama kaua, kui kliendil on lennufirma juures konto.

Kuna isikutuvastusandmeid ja biomeetrilisi andmeid säilitatakse pilves asuvas keskses andmebaasis, võib sellistele andmetele olla juurdepääs mitmel üksusel, sealhulgas võib-olla ka EMP-välistel teenuseosutajatel. Reisija andmed dekrüpteeritakse ja krüpteerimisvõtmed on lennufirma või tema töötlejate kontrolli all, mis võib suurendada turvaohte. Selline tsentraliseeritud säilitusarhitektuur tähendab ka seda, et reisija kontroll oma andmete üle üha väheneb. Andmeid võidakse säilitada ka pika aja jooksul, mis toob kaasa suurema andmetega seotud rikkumise ohu ning näib ulatuvat kaugemale sellest, mis on töötlemise eesmärgil rangelt vajalik ja proportsionaalne, välja arvatud juhul, kui üksikisikutele avalduva ohu leevendamiseks võetakse täiendavaid meetmeid.

Andmekaitsenõukogu leiab, et sarnast tulemust lennujaamades reisijatevoo sujuvamaks muutmisel on võimalik saavutada vähem sekkuval viisil ning negatiivne mõju andmesubjektide põhiõigustele ja -vabadustele, mis võib tuleneda andmetega seotud rikkumisest biomeetriliste andmete keskandmebaasis, näib kaaluvat üles töötlemisest tuleneva eeldatava kasu. Seetõttu ei vasta töötlemine vajalikkuse ja proportsionaalsuse põhimõtetele. Selle põhjal järeldab andmekaitsenõukogu, et neljandas stsenaariumis ette nähtud töötlemist **ei saa lugeda isikuandmete kaitse üldmääruse artikliga 25 kooskõlas olevaks**. Samuti **ei oleks see** andmekaitsenõukogule teadaoleva teabe kohaselt **kooskõlas isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktiga e** ega **isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktiga f ja artikliga 32**, kui vastutav töötleja selles stsenaariumis kirjeldatud meetmetega piirdukski.

Sisukord

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) (edaspidi „**IKÜM**“) artiklit 63 ja artikli 64 lõiget 2,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

Võttes arvesse Euroopa Andmekaitsenõukogu (edaspidi „**EAKN**“) töökorra artikleid 10 ja 22,

ning arvestades järgmist:

(1) Andmekaitsenõukogu peamine ülesanne on tagada IKÜM järjepidev kohaldamine kogu Euroopa Majanduspiirkonnas (edaspidi „**EMP**“). IKÜM artikli 64 lõikes 2 on sätestatud, et pädev järelevalveasutus, andmekaitsenõukogu eesistuja või Euroopa Komisjon võib taotleda mis tahes üldkohaldatava või rohkem kui ühes EMP liikmesriigis mõju avaldava küsimuse puhul, et seda käsitleks arvamuse esitamiseks andmekaitsenõukogu.

(2) Andmekaitsenõukogu arvamus võetakse vastu vastavalt IKÜM artikli 64 lõikele 3 koostoimes EAKN töökorra artikli 10 lõikega 2 kaheksa nädala jooksul pärast seda, kui eesistuja on otsustanud, et toimik on täielik. Eesistuja otsusel võib seda ajavahemikku pikendada kuue nädala võrra, võttes arvesse küsimuse keerukust,

on vastu võtnud järgmise arvamuse:

1 SISSEJUHATUS

1.1 Faktiliste asjaolude kokkuvõte

1. 16. veebruaril 2024 palus Prantsusmaa järelevalveasutus (edaspidi „Prantsusmaa JVA“) andmekaitsenõukogul esitada arvamuse selle kohta, kas IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32 on kooskõlas näotuvastustehnoloogia kasutamine lennujaama käitajate ja lennuettevõtjate poolt reisijate[2] biomeetriliseks autentimiseks või tuvastamiseks, et muuta reisijatevood lennujaama julgestuskontrollis sujuvamaks [3], pagasi äraandmisel, pardaleminekul ja reisijate *lounge*'ile juurdepääsul (v.a piirikontrollidel ja tollimaksuvabade kaupluste tehtavatel kontrollidel) (edaspidi „taotlus“). Prantsusmaa JVA lisas oma taotlusele tüüpiliste näidisjuhtumite kirjelduse (I lisa).

[1] Käesolevas arvamuses sisalduvaid viiteid liikmesriikidele tuleks mõista kui viiteid EMP liikmesriikidele. Käesolevas arvamuses sisalduvaid viiteid liidule või EL-ile tuleks mõista kui viiteid EMP-le.

[2] Käesolevas arvamuses tähendab „**reisija**“ andmesubjekti, kelle isikuandmeid töödeldakse käesolevas arvamuses kirjeldatud konkreetsel eesmärgil. Käesolevas ettepanekus kasutatakse mõisteid „reisija“ ja „üksikisik“ sünonüümidena.

[3] Käesolevas arvamuses on „**lennujaama julgestuskontroll**“ lennujaama käitaja vastutusel tehtav julgestuskontroll, mille reisijad peavad läbima selleks, et siseneda väljuvate lendude saalist pardalemineku alasse või väravasse.

2. Prantsusmaa JVA märgib oma taotluses, et mudelid, mida praegu mitmes ELi lennujaamas testitakse, on liikmesriigiti erinevad, mis võib tekitada ohu, et järelevalveasutuste tõlgendused erinevad, ning ohu, et ELi andmesubjektide põhiõigustele ja -vabadustele tekivad erinevad mõjud[4].

3. Andmekaitsenõukogu leiab, et taotlusele vastamiseks on vaja vastata järgmistele küsimustele.

4. **1. küsimus**:

1.1. Kas näotuvastustehnoloogia kasutamine biomeetrilise autentimise eesmärgil **reisijatevoo sujuvamaks muutmiseks lennujaamades** (julgestuskontroll, pagasi äraandmine, pardaleminek ja juurdepääs reisijate *lounge*'ile) on kooskõlas **IKÜM artikli 5 lõike 1 punktiga f, artiklitega 25 ja 32**, kui tegemist on säilitusarhitektuuriga, mille puhul iga reisija biomeetriline mall asub **ainult üksikisiku valduses**, nt tema individuaalses seadmes, mis on tema ainukontrolli all?

1.2. Kui sellist töötlemist pidada eespool nimetatud sätetega kooskõlas olevaks, siis milliseid miinimum asjakohaseid kaitsemeetmeid oleks IKÜM artikleid 25 ja 32 silmas pidades vaja?

2. küsimus:

2.1. Kas näotuvastustehnoloogia kasutamine biomeetrilise autentimise või tuvastamise eesmärgil **reisijatevoo ühtlustamiseks lennujaamades** (julgestuskontroll, pagasi äraandmine, pardaleminek ja juurdepääs reisijate *lounge*'ile) on kooskõlas **IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32**, kui tegemist on **tsentraliseeritud säilitusarhitektuuriga**, mille puhul iga reisija biomeetriline mall asub keskses andmebaasis:

2.1.1. lennujaama keskandmebaasis, lennujaama käitaja kontrolli all, krüpteeritud kujul, ning võti/saladus on üksnes üksikisiku valduses (näiteks üksikisiku mobiiltelefonis) (autentimise jaoks)?

2.1.2. Kui sellist töötlemist pidada kooskõlas olevaks, siis milliseid minimaalseid asjakohaseid kaitsemeetmeid oleks IKÜM artikleid 25 ja 32 silmas pidades vaja?

2.2.1. lennujaama keskandmebaasis, lennujaama käitaja kontrolli all, krüpteeritud kujul koos lennujaama käitaja valduses olevate võtmetega (tuvastamise jaoks)?

2.2.2. Kui sellist töötlemist pidada kooskõlas olevaks, siis milliseid minimaalseid asjakohaseid kaitsemeetmeid oleks IKÜM artikleid 25 ja 32 silmas pidades vaja?

2.3.1. pilveteenuses lennufirma või tema teenuseosutaja (volitatud töötleja) kontrolli all, krüpteeritud kujul, võtmed on lennufirma või tema teenuseosutaja valduses (tuvastamise jaoks)?

2.3.2. Kui sellist töötlemist pidada kooskõlas olevaks, siis milliseid minimaalseid asjakohaseid kaitsemeetmeid oleks IKÜM artikleid 25 ja 32 silmas pidades vaja?

[4] Taotlus, lk 1.

5. Pärast seda, kui Prantsusmaa järelevalveasutus 16. veebruaril 2024 otsustas, et toimik on täielik ja andmekaitsenõukogu esimees 23. veebruaril 2024 selle täielikkust kinnitas, edastas sekretariaat toimiku 23. veebruaril 2024. Andmekaitsenõukogu esimees otsustas kooskõlas IKÜM artikli 64 lõikega 3 koostoimes Euroopa Andmekaitsenõukogu töökorra artikli 10 lõikega 2 pikendada küsimuse keerukuse tõttu algset kaheksanädalast tähtaega veel kuue nädala võrra.

1.2 IKÜM artikli 64 lõike 2 alusel esitatud arvamustaotluse vastuvõetavus

6. IKÜM artikli 64 lõikes 2 on nimelt sätestatud, et iga järelevalveasutus võib taotleda mis tahes üldkohaldatava või rohkem kui ühes liikmesriigis mõju avaldava küsimuse puhul, et seda käsitleks arvamuse esitamiseks andmekaitsenõukogu.

7. Andmekaitsenõukogu leiab, et Prantsusmaa JVA esitatud taotlus lennujaamades reisijatevoo sujuvamaks muutmise eesmärgil näotuvastustehnoloogia kasutamise kohta biomeetriliste andmete autentimiseks või tuvastamiseks on seotud küsimustega, millel on mõju rohkem kui ühes liikmesriigis, sest nagu taotluses[5] on selgitatud, on liikmesriikide lennujaamades käimas mitmeid projekte ja hinnangute kohaselt selline lähenemisviis lähiaastatel üha levib. Mudelid, mida erinevad lennujaamad ja lennufirmad praegu katsetatavad on liikmesriigiti väga erinevad, mis võib tekitada ohu, et mõju andmekaitsele lahkneb rohkem kui ühes liikmesriigis.

8. Samuti leiab andmekaitsenõukogu, et Prantsusmaa JVA esitatud taotlusel on olulised tagajärjed IKÜM artikli 5 lõike 1 punktides e ja f sätestatud põhimõtete ning IKÜM artikli 25 alusel vastutavate töötlejate suhtes kohaldatavate nõuete ning IKÜM artikli 32 alusel vastutavate töötlejate ja volitatud töötlejate suhtes kohaldatavate nõuete kohaldamisele. Seetõttu puudutab käesolev taotlus „üldkohaldatavat küsimust“ IKÜM artikli 64 lõike 2 tähenduses, kuna see on seotud säilitamise piirangu (IKÜM artikli 5 lõike 1 punkt e) ning usaldusväärsuse ja konfidentsiaalsuse (IKÜM artikli 5 lõike 1 punkt f) põhimõtete ning lõimitud ja vaikimisi andmekaitse (IKÜM artikkel 25) ja andmete turvalisuse (IKÜM artikkel 32) põhimõtete ühetaolise tõlgendamisega, et tagada muu hulgas nende sätete järjepidev kohaldamine EMPs.

9. Liikmesriikide võimalikud lahknevad seisukohad IKÜM artikli 5 lõike 1 punktide e ja f ning artiklite 25 ja 32 tõlgendamisel suurendaksid ohtu, et lennujaamade käitajad ja lennufirmad arendavad näotuvastusprojekte ebaühtlaselt. Kuna Prantsusmaa JVA on välja toonud selge vajaduse tõlgendada ühetaoliselt neid sätteid seoses lennujaamades reisijatevoo sujuvamaks muutmisel kasutatava reisijate biomeetrilise autentimise või tuvastamise näotuvastustehnoloogiaga[6], leiab andmekaitsenõukogu kooskõlas Euroopa Andmekaitsenõukogu töökorra artikli 10 lõikega 3, et taotlus on põhjendatud.

10. IKÜM artikli 64 lõike 3 kohaselt ei pea Euroopa Andmekaitsenõukogu arvamust esitama, kui ta on oma arvamuse selles küsimuses juba esitanud[7]. Andmekaitsenõukogu ei ole veel Prantsusmaa JVA taotlusest tulenevatele küsimustele vastanud. Kuigi Euroopa Andmekaitsenõukogu suunistes 3/2019

[5] Taotlus, lk 3.
[6] Taotlus, lk 1–3.
[7] Isikuandmete kaitse üldmääruse artikli 64 lõige 3 ja Euroopa Andmekaitsenõukogu töökorra artikli 10 lõige 4.

videoseadmete kohta[8] on juba esitatud mõned kasulikud elemendid turvameetmete kohta, mida tuleks biomeetriliste andmete töötlemisel kohaldada, ei käsitleta neis kõiki taotluses tõstatatud küsimustega seotud aspekte. Lisaks ei sisalda kättesaadavad Euroopa Andmekaitsenõukogu suunised, sealhulgas Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, konkreetseid suuniseid võimalike elementide kohta, mida tuleb kontrollida seoses lennujaamades reisijatevoo sujuvamaks muutmisel reisijate tuvastamiseks või autentimiseks kasutatavate biomeetriliste andmete tsentraliseeritud või detsentraliseeritud säilitamisega, ega selle kohta, kas selline töötlemine on kooskõlas IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32.

11. Neil põhjustel leiab andmekaitsenõukogu, et taotlus on vastuvõetav ja selles tõstatatud küsimusi tuleks analüüsida IKÜM artikli 64 lõike 2 kohaselt vastu võetavas arvamuses.

2 ARVAMUSE ULATUS JA KONTEKST

2.1 ARVAMUSE ULATUS

12. Käesolev arvamus käsitleb üksnes seda, kas näotuvastustehnoloogia kasutamine lennujaama käitajate ja lennufirmade poolt reisijate biomeetriliseks autentimiseks või tuvastamiseks, **et muuta lennujaamas reisijatevood sujuvamaks ,** nimelt julgestuskontrollis, pagasi äraandmisel, pardaleminekul ja reisijate *lounge*'ile juurdepääsul on kooskõlas IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32.

13. Seoses käesoleva **arvamuse käsitlusalaga** selgitab andmekaitsenõukogu järgmist.

    1) Isikuandmete töötlemine piirikontrolli ja tollimaksuvabade kaupluste tehtavate kontrollide raames ei kuulu käesoleva arvamuse käsitlusalasse, kuna seda teevad muud vastutavad töötlejad kui lennujaama käitajad ja lennufirmad.

    2) Näotuvastustehnoloogia kasutamine muudel eesmärkidel (nt õiguskaitse) või mis tahes muu isiku poolt, isegi kui see toimub sarnastel eesmärkidel ja põhineb allpool jaotises 3.2 kirjeldatud stsenaariumidel, ei kuulu käesoleva ettepaneku kohaldamisalasse.

    3) Käesolevas arvamuses käsitletakse üksnes reisijate isikuandmete töötlemist ja see ei hõlma muud liiki andmesubjekte, nagu lennujaamakäitajate või lennufirmade töötajad.

    4) Käesolevas arvamuses analüüsitakse Prantsusmaa JVA esitatud taotlust seoses sellega, kas reisijate biomeetriliste mallide säilitusarhitektuur on kooskõlas IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32. Seda silmas pidades ei sisalda käesolev arvamus täielikku analüüsi selle kohta, kas asjaomane(asjaomased) vastutav(ad) töötleja(d) ja vajaduse korral nende volitatud töötleja(d) järgivad IKÜMit. See on eriti oluline, arvestades, et nende tehnoloogiatega kaasnevad suuremad ohud seoses eriliiki andmete töötlemisega vastavalt IKÜM artiklile 9. Seetõttu ei piira käesolev arvamus näotuvastustehnoloogiate kasutamise hindamist vastavalt

[8] Euroopa Andmekaitsenõukogu suunised 3/2019 isikuandmete töötlemise kohta videoseadmetes, versioon 2.0, vastu võetud 29. jaanuaril 2020 (edaspidi „**Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta**").

muudele IKÜMi sätetele, sealhulgas taotluses käsitletud konkreetses valdkonnas, ega juhtumipõhist õiguslikku ja tehnilist analüüsi, mis põhineb vastutava töötleja konkreetsel kavandatud töötlemisel ja asjaoludel.

5) Käesolevas arvamuses ei käsitleta laste isikuandmete töötlemist ega piirata sellega seoses kohaldatavaid erinõudeid.

6) Käesolev arvamus ei piira liikmesriikide siseriiklikest õigusaktidest tulenevaid õiguslikke nõudeid ega täiendavaid piiranguid biomeetriliste andmete kasutamisele[9].

7) Käesolevas ettepanekus esitatud järeldused ei piira tehnoloogia edasist arengut.

8) Käesolevas arvamuses käsitletakse nelja stsenaariumi, mille erisusi on kirjeldatud allpool jaotises 3.2. Selles ei käsitleta muid stsenaariume, isegi kui töötlemine toimub samal eesmärgil.

14. Prantsusmaa JVA märkis oma taotluses, et reisijate biomeetriliste andmete töötlemine lennujaamades reisijatevoo sujuvamaks muutmise eesmärgil põhineb eeldusel, et üksikisikud on sellise töötlemisega nõus, mis võib olla IKÜMist tulenev õiguslik alus[10]. **Kuid andmekaitsenõukogule taotluses esitatud küsimused <u>ei hõlma</u> kohaldatava <u>õigusliku aluse</u> analüüsi ja seetõttu <u>ei analüüsita käesolevas arvamuses selliseks töötlemiseks antud nõusoleku kehtivust kooskõlas IKÜM artiklitega 6, 7 ja 9</u>.**

15. Andmekaitsenõukogu märgib siiski üldiselt, et kui asjaomased vastutavad töötlejad tugineksid sellele õiguslikule alusele, peaksid nad saama selliseid teenuseid kasutada soovivatelt isikutelt kehtiva selgesõnalise nõusoleku[11]. Selline selgesõnaline nõusolek peab olema vabatahtlik, konkreetne ja teadlik[12] ning seda, kas need tingimused on täidetud, analüüsitakse iga juhtumi puhul eraldi. See tähendab muu hulgas, et:

1) Üksikisikud peaksid saama sellise nõusoleku igal ajal ja ilma kahjulike tagajärgedeta hõlpsasti tagasi võtta[13].

2) Selleks et nõusolek oleks vabatahtlik, võib biomeetrilisi tehnoloogiaid kasutada üksnes vabatahtlikkuse alusel, sest üksikisikud peaksid saama vabalt valida, kas neid teenuseid kasutada või mitte, ilma et sellega kaasneks kahjulikud tagajärjed (näiteks

[9] Näiteks on isikuandmete kaitse üldmääruse artikli 9 lõikes 4 sätestatud, et liikmesriigid võivad säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses biomeetriliste andmete töötlemisega.
[10] Taotluse I lisa.
[11] Isikuandmete kaitse üldmääruse artikli 4 punkti 14 ja artikli 9 lõike 1 ning artikli 9 lõike 2 punkti a kohaselt on keelatud biomeetriliste andmete töötlemine füüsilise isiku kordumatuks tuvastamiseks, välja arvatud juhul, kui andmesubjekt on andnud selgesõnalise nõusoleku nende isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil, välja arvatud juhul, kui liidu või liikmesriigi õiguse kohaselt ei saa andmesubjekt ei või isikuandmete kaitse üldmääruse artikli 9 lõikes 1 nimetatud keeldu tühistada. Vt ka isikuandmete kaitse üldmääruse põhjendused 51, 52 ja 53.
[12] Isikuandmete kaitse üldmääruse artikli 4 lõige 11 ja artikkel 7.
[13] Isikuandmete kaitse üldmääruse artikli 7 lõige 4, samuti põhjendus 50.

märkimisväärselt pikemad viivitused reisijatele, kes ei anna nõusoleku[14]), stiimulid, lisakulud või muud vastutasuks pakutavad soodustused[15].

3) Selgesõnalist nõusolekut tuleks küsida ka isikutelt, kelle biomeetrilisi andmeid töödeldakse, isegi kui nad ei ole selliste vahendite abil tuvastamiseks või autentimiseks registreerunud. Teisisõnu on oluline, et isikute nägusid, kes ei ole näotuvastusega kavandatud eesmärgile sõnaselge nõusoleku andnud, kaameraga ei skaneeritaks. Seda on võimalik saavutada näiteks spetsiaalsete näotuvastuskoridoride loomise ning asjakohaste märgiste ja füüsilise eraldamisega mittebiomeetriliselt kontrollitavatest reisijavoogudest, nii et sellised koridorid oleksid selgelt tuvastatavad.

4) Ilma et see piiraks seda, kas nõusolek oleks sellise töötlemise suhtes kohaldatav õiguslik alus, kohaldatakse IKÜM artiklis 5 sätestatud töötlemise põhimõtteid seoses vajalikkuse ja proportsionaalsusega siiski ka siis, kui üksikisikud on andnud oma selgesõnalise nõusoleku oma biomeetriliste andmete kasutamiseks[16].

16. Taotluses täpsustatakse[17], et lennujaama julgestuskontrollipunktides toimuva töötlemise puhul on vastutavad töötlejad lennujaama käitajad, samas kui pagasi äraandmise, pardalemineku ja reisijate *lounge*'ile juurdepääsu puhul on vastutavad töötlejad lennufirmad. Andmekaitsenõukogu märgib, et seega võivad taotluses kirjeldatud töötlemisse olla kaasatud erinevad osalejad ning ta ei ole käesoleva arvamuse jaotises 3.2 kirjeldatud stsenaariumide puhul (kaas)vastutava töötleja ja/või volitatud töötleja rolli hinnanud. Iga juhtumi puhul tuleb asjaomased osalejad kindlaks määrata ja nende kohustused selgelt jaotada, et IKÜMi nõuded oleksid täidetud[18].

17. Lisaks märgib andmekaitsenõukogu, et praegu puuduvad ELis ühtsed õiguslikud nõuded, millest lähtudes lennujaama käitajad ja lennufirmad peaksid kõigis eespool nimetatud kontrollpunktides reisijaid tuvastama ja kontrollima, kas reisija pardakaardil olev nimi vastab nende isikut tõendaval dokumendil olevale nimele[19]. Seega kohaldatakse selliste nõuete suhtes siseriiklikke õigusakte, mis võivad liikmesriigiti erineda. Mõnes liikmesriigis võib selline kontroll olla nõutav mõne kontrollpunkti puhul (nt pagasi äraandmine või pardaleminek), samas kui teistes liikmesriikides sellist kontrolli

[14] Siin võiks kaaluda näiteks sellise süsteemi väljatöötamist, mis ei survesta sotsiaalselt reisijaid, kes ei soovi nõusolekut anda. Samuti ei tohiks selliste reisijate valikud mõjutada negatiivselt teisi reisijaid.

[15] Euroopa Andmekaitsenõukogu suunised 05/2020 määruse 2016/679 kohase nõusoleku kohta, versioon 1.1, vastu võetud 4. mail 2020 (edaspidi „**Euroopa Andmekaitsenõukogu suunised 5/2020, nõusoleku kohta**"), punktid 46 ja 48.

[16] Samas, punkt 5.

[17] Taotluse I lisa.

[18] Kooskõlas isikuandmete kaitse üldmääruse artikli 4 lõigetega 7 ja 8, artikli 5 lõikega 2 ning artiklitega 24, 26, 28 ja 29. Vt ka Euroopa Andmekaitsenõukogu suunised 07/2020 vastutava töötleja ja volitatud töötleja mõistete kohta isikuandmete kaitse üldmääruses, versioon 2.1, vastu võetud 7. juulil 2021.

[19] Asjaomane ELi tasandi määrus on komisjoni 5. novembri 2015. aasta rakendusmäärus (EL) 2015/1998, millega nähakse ette lennundusjulgestuse ühiste põhistandardite rakendamise üksikasjalikud meetmed. Selles määruses ei käsitleta aga ametlike isikut tõendavate dokumentide kontrollimist lennujaamade kontrollpunktides ning liikmesriikidel on õigus seda reguleerida riiklikul tasandil.

praegu ei nõuta[20]. Erinevate lennujaamade tavasid reisijate isikusamasuse kontrollimisel mõjutab otseselt õiguslike kohustuste olemasolu.

18. Seetõttu ei tohiks **biomeetrilist kontrolli teha** sellistes olukordades, **kus reisijate isikusamasuse kontrollimine ametliku isikut tõendava dokumendiga ei ole nõutud, , sest see tooks kaasa ülemäärase andmetöötlemise, kuna võrreldes praeguse olukorraga tuleks töödelda täiendavaid andmeid, ja läheks kaugemale sellest, mis on vajalik asjaomase eesmärgi saavutamiseks, rikkudes sellega IKÜM artikli 5 lõike 1 punktis c sätestatud võimalikult väheste andmete kogumise põhimõtet.** Seda kaalutlust tuleb arvesse võtta kõigi allpool käesoleva ettepaneku jaotises 3.2 kirjeldatud stsenaariumide analüüsimisel.

2.2 Põhimõisted

19. Selleks, et kvalifitseeruda IKÜM artikli 4 lõikes 14[21] määratletud biomeetrilisteks andmeteks, peaks selliste toorandmete töötlemine nagu füüsilise isiku füüsilised, füsioloogilised või käitumuslikud omadused hõlmama nende omaduste mõõtmist, kuna biomeetrilised andmed saadakse selliste mõõtmiste tulemusel[22].

20. Isiku näo kujutisest (foto või video), mida nimetatakse biomeetriliseks „**näidiseks**“, saadakse näo eri omaduste digitaalne väljendus (seda nimetatakse „**malliks**“)[23]. Lisaks tuletab andmekaitsenõukogu meelde, et „[b]iomeetriline mall on biomeetrilistest näidistest saadud kordumatute omaduste digitaalne väljendus, mida saab säilitada biomeetrilises andmebaasis“[24] ja mis võimaldab kõnealust füüsilist isikut kordumatult tuvastada või kinnitada tema isiku tuvastamist. Lisaks „[p]eab see biomeetriline mall olema kordumatu ja igale üksikisikule ainuomane ning see on põhimõtteliselt aja jooksul püsiv“[25]. Võrdlusprotsessi käigus, mille eesmärk on isiku tuvastamine või autentimine näotuvastuse abil, võrreldakse harilikult sissetulevat biomeetrilist malli salvestatud tunnustega, et kontrollida kokkulangevust või leida see andmebaasis[26].

---

[20] See tähendab, et praegu kontroll puudub täiesti või kontrollitakse üksnes pardakaardi olemasolu. Näiteks vastavalt 22. mai 1954. aasta protokollile, milles käsitletakse Taani, Soome, Norra ja Rootsi kodanike vabastamist kohustusest omada passi või elamisluba, kui nad elavad Skandinaavia riigis, mis ei ole nende päritoluriik, on Norra, Taani, Soome ja Rootsi kodanikud alates 1. juulist 1954 vabastatud kohustusest kanda nende riikide vahel reisides kaasas passi või muud isikut tõendavat dokumenti.

[21] Vt ka isikuandmete kaitse üldmääruse põhjendused 51, 52 ja 53.

[22] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 74.

[23] Euroopa Andmekaitsenõukogu suunised 05/2022 näotuvastustehnoloogia kasutamise kohta õiguskaitse valdkonnas, versioon 2.0, vastu võetud 26. aprillil 2023 (edaspidi „**Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses**“), punktid 7 ja 8.

[24] Samas, punkt 9.

[25] Samas.

[26] Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses, punktid 10–11; vt ka rahvusvaheline standard ISO/IEC 2382–37, 2022–03, kättesaadav aadressil https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [viimati vaadatud 23. mail 2024] (edaspidi „**ISO/IEC 2382-37**“)

21. Näotuvastustehnoloogia võib täita kahte erinevat funktsiooni: autentimine[27] ja tuvastamine[28]. Kuigi tegu on erinevate funktsioonidega, on mõlema aluseks tuvastatud või tuvastatava füüsilise isikuga seotud biomeetriliste andmete[29]töötlemine ja seega on tegu eriliiki isikuandmete töötlemisega IKÜM artikli 9 tähenduses[30].

22. Eelkõige tuleb silmas pidada järgmist.

> **Autentimise** eesmärk on kinnitada biomeetrilist väidet võrdlemise teel. Seda nimetatakse ka üks-ühele kontrolliks.
>
> **Tuvastamise** eesmärk on teha otsing biomeetriliste registreeringute andmebaasist, et leida konkreetsele isikule omased tunnused. Seda nimetatakse ka üks-mitmele tuvastamiseks.

23. Mõlema protsessi (st tuvastamine ja autentimine) puhul põhinevad näotuvastusmeetodid mallide (st võrreldava ja võrdlusalus(t)e) hinnangulisel kokkulangevusel. Sellest seisukohast põhinevad mõlemad tõenäosusel: võrdluse tulemusel saadakse suurem või väiksem tõenäosus, et isik on tõepoolest autenditav või tuvastatav isik; kui see tõenäosus ületab süsteemis teatava künnise, mille on kindlaks määranud süsteemi kasutaja või arendaja, eeldab süsteem, et on leitud tuvastatav või autenditav kokkulangevus[31].

[27] Andmekaitsenõukogu märgib, et tulevases Euroopa Parlamendi ja nõukogu määruses, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellektimäärus) (*Euroopa Liidu Teatajas* seni avaldamata), on artikli 3 punktis 36 määratletud ka mõiste „biomeetriline kontroll“ kui „füüsiliste isikute isikusamasuse automaatne, üks-ühele kontrollimine, sealhulgas autentimine, võrreldes nende biomeetrilisi andmeid varem esitatud biomeetriliste andmetega“ (vt Euroopa Parlamendi 13. märtsi 2024. aasta seadusandlik resolutsioon ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud normid (tehisintellektimäärus) ja muudetakse teatavaid liidu õigusakte (COM(2021)0206 – C9–0146/2021–2021/0106(COD)).

[28] Samas, tehisintellekti käsitleva õigusakti artikli 3 punktis 35 on „biomeetriline tuvastamine“ määratletud kui „inimese füüsiliste, füsioloogiliste, käitumuslike või psühholoogiliste omaduste automaatne tuvastamine füüsilise isiku isikusamasuse kindlakstegemiseks, võrreldes isiku biomeetrilisi andmeid andmebaasis säilitatavate isikute biomeetriliste andmetega“.

[29] ISO/IEC 2382-37.

[30] Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses, artikli 4 lõige 14 punkt 12.

[31] Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses, punkt 11. Vt ka ISO/IEC 2382-37.

3 TAOTLUSE SISULINE LÄBIVAATAMINE

3.1 Üldised märkused

24. Käesolevas jaotises analüüsitakse eespool punktis 4 esitatud küsimusi. Sellega seoses analüüsib andmekaitsenõukogu esimese küsimuse puhul kooskõla IKÜM artikli 5 lõike 1 punktiga f ning artiklitega 25 ja 32 ning teise küsimuse puhul kooskõla IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32.

25. Selleks analüüsib andmekaitsenõukogu nelja erinevat stsenaariumi[32], mille eriomadusi on kirjeldatud allpool jaotises 3.2.

26. Sissejuhatava märkusena tuletab andmekaitsenõukogu meelde, et biomeetriliste andmete ja eelkõige näotuvastustehnoloogia kasutamine kujutab endast suurenenud ohtu andmesubjektide õigustele ja vabadustele. Esmajoones puudutab selline töötlemine biomeetriliste andmete töötlemist. Biomeetrilised andmed on IKÜM artikli 9 alusel erilise kaitse all. Eelkõige muudavad biomeetrilised andmed pöördumatult keha ja identiteedi vahelist seost, kuna need muudavad inimkeha omadused „masinloetavaks“ ja neid võidakse kasutada edaspidi muul otstarbel[33]. Lisaks võib näotuvastustehnoloogia kasutamine põhjustada valenegatiivsete tulemuste, kallutatuse ja diskrimineerimisega seotud ohte[34] ning biomeetriliste andmete võimalikul väärkasutamisel võivad olla üksikisikutele tõsised tagajärjed, näiteks identiteedipettus või kellegi teisena esinemine[35]. Samuti tuleks märkida, et kui näotuvastus toimub kaugmeetodil ja ilma andmesubjekti aktiivse osaluseta, võivad üksikisikud olla sellisest töötlemisest ja sellega seotud ohtudest veelgi vähem teadlikud. Lõpetuseks on oluline rõhutada, et tunnuseid, millel biomeetrilised andmed põhinevad, võib üldiselt pidada püsivateks ja neid ei saa tühistada, eriti näotuvastuse kontekstis[36].

27. Seetõttu peaksid vastutavad töötlejad enne selliste tehnoloogiate kasutamist, isegi kui neid peetakse eriti tõhusaks, hindama mõju andmesubjektide põhiõigustele ja -vabadustele ning kaaluma, kas töötlemise õiguspärast eesmärki saaks saavutada vähem sekkuvate vahenditega[37].

---

[32] Neli andmekaitsenõukogu analüüsitud stsenaariumi põhinevad taotluse I lisas esitatud kasutusjuhtudel. Prantsusmaa järelevalveasutus on selgitanud, et taotluse I lisas esitatud kasutusjuhud on näited stsenaariumide rakendamise kohta ja neid kasutatakse näitlikel eesmärkidel.

[33] Artikli 29 töörühma arvamus 3/2012 biomeetriliste tehnoloogiate arengu kohta, vastu võetud 27. aprillil 2012, WP193 (edaspidi „**artikli 29 töörühma arvamus 3/2012 biomeetriliste tehnoloogiate kohta**“), lk 4. Tuleb märkida, et käesolevas arvamuses viidatakse 24. oktoobri 1995. aasta direktiivile 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (edaspidi „andmekaitsedirektiiv“). Isikuandmete kaitse üldmäärusega on laiendatud andmete eriliikide kohaldamisala ja erinevalt andmekaitsedirektiivist on isikuandmete kaitse üldmääruses sätestatud, et biomeetrilised andmed on andmete eriliigid (isikuandmete kaitse üldmääruse artikkel 9).

[34] Suunised näotuvastuse kohta, Euroopa Nõukogu isiku kaitset isikuandmete automatiseeritud töötlemisel käsitleva konventsiooni konsultatiivkomitee, juuni 2021, lk 15; samuti Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses, punkt 27.

[35] Artikli 29 töörühma arvamus 3/2012 biomeetriliste tehnoloogiate kohta, lk 29.

[36] Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses, punkt 104.

[37] Isikuandmete kaitse üldmääruse põhjendus 39. Vt ka Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 73.

28. Andmekaitsenõukogu tuletab samuti meelde, et õigus isikuandmete kaitsele ei ole absoluutne õigus ja seda tuleks tasakaalustada muude hartaga kaitstud põhiõigustega vastavalt proportsionaalsuse põhimõttele[38].

29. IKÜM[39] artikli 25 lõikes 1 osutatakse IKÜM artiklis 5 loetletud andmekaitsepõhimõtetele ja nõutakse nende lõimitud „tõhusat“[40] rakendamist. See hõlmab sõnaselgelt IKÜM[41] artikli 5 lõike 1 punktis c sätestatud võimalikult väheste andmete kogumise põhimõtet, mille kohaselt peavad isikuandmed olema „asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt, järgides proportsionaalsuse põhimõtet“[42]. Lisaks on IKÜM artikli 25 lõikes 2 sätestatud kohustus koguda „vaikimisi võimalikult väheseid andmeid“. See kehtib kogutud isikuandmete hulga, nende töötlemise ulatuse, nende säilitamise aja ja nende kättesaadavuse suhtes[43].

30. IKÜM artiklis 25 ei nõuta siiski, et vastutavad töötlejad rakendaksid konkreetseid tehnilisi ja korralduslikke meetmeid, vaid pigem nõutakse, et valitud meetmed ja kaitsemeetmed oleksid asjakohased töötlemisest tulenevate andmesubjekti õigusi ja vabadusi ähvardavate ohtude seisukohast[44]. Samamoodi nõutakse IKÜM artiklis 32, mis käsitleb isikuandmete töötlemise turvalisust, et vastutav töötleja ja volitatud töötleja rakendaksid asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada vastav turvalisuse tase füüsiliste isikute õigustele ja vabadustele tekkida võivale ohule.

---

[38] Isikuandmete kaitse üldmääruse põhjendus 4. Vt selle kohta ka kohtuotsus, Euroopa Kohus, 22. juuni 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (edaspidi „C-439/19 Latvijas Republikas Saeima“), punktid 98, 110 ja 113. Lisaks nõuab liidu õiguse üldpõhimõtete hulka kuuluv proportsionaalsuse põhimõte, et liidu õigusaktidega rakendatud meetmed oleksid taotletava eesmärgi saavutamiseks sobivad ega läheks kaugemale sellest, mis on eesmärgi saavutamiseks vajalik (vt kohtuotsus, Euroopa Kohus, 9. november 2010, *Volker und Markus Schecke ja Eifert*, C-92/09 ja C-93/09, ECLI:EU:C:2010:662 (edaspidi „C-92/09 ja C-93/09 *Volker und Schecke*“), punkt 74 ja seal viidatud kohtupraktika).

[39] Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, versioon 2.0, vastu võetud 20. oktoobril 2020 (edaspidi „**Euroopa Andmekaitsenõukogu suunised 4/2019 lõimitud ja vaikimisi andmekaitse kohta**“), punkt 11.

[40] Isikuandmete kaitse üldmääruse artikli 25 lõikes 1 on öeldud: „Võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning töötlemise laadi, ulatust, konteksti ja eesmärke, samuti töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte, rakendab vastutav töötleja nii töötlemisvahendite kindlaksmääramisel kui ka isikuandmete töötlemise ajal asjakohaseid tehnilisi ja korralduslikke meetmeid, nagu pseudonümiseerimine, mis on vajalikud andmekaitsepõhimõtete (nagu võimalikult väheste andmete kogumine) tõhusaks rakendamiseks ja vajalike kaitsemeetmete lõimimiseks isikuandmete töötlemisse, et täita käesoleva määruse nõudeid ja kaitsta andmesubjektide õigusi.“ Vt Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, punkt 13.

[41] Isikuandmete kaitse üldmääruse põhjenduses 39 on sätestatud, et isikuandmeid tuleks töödelda vaid juhul, kui nende töötlemise eesmärki ei ole mõistlikult võimalik saavutada muude vahendite abil.

[42] Kohtuasi C-439/19: *Latvijas Republikas Saeima*, punkt 98; kohtuotsus, Euroopa Kohus, 11. detsember 2019, *Asociaťia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (edaspidi „C-708/18 *M5A-ScaraA*“), punkt 48.

[43] Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, lk 48.

[44] Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, lk 14.

31. Oluline on see, et isegi kui reisijad annavad sõnaselge nõusoleku oma biomeetriliste andmete kasutamiseks lennujaamades reisijatevoo sujuvamaks muutmise eesmärgil, kohaldatakse ja tuleb järgida IKÜMis sätestatud vajalikkuse ja proportsionaalsuse põhimõtteid[45].

32. **Vajalikkuse põhimõtte** puhul kaalub andmekaitsenõukogu, kas kavandatav töötlemine on vajalik taotletava eesmärgi saavutamiseks ning kas sama eesmärki on võimalik saavutada sama tõhusalt muude vahenditega, mis riivavad vähem andmesubjekti põhiõigusi ja -vabadusi[46]. Seoses **proportsionaalsuse põhimõttega** hindab andmekaitsenõukogu, kas negatiivne mõju andmesubjektide põhiõigustele ja -vabadustele on proportsionaalne eeldatava kasuga. Kui kasu on suhteliselt väike, ei pruugi selline mõju olla proportsionaalne[47].

33. Isegi kui andmekaitsenõukogu leiab, et üks allpool analüüsitud stsenaariumidest võib vastata IKÜM artikli 5 lõike 1 punktide e ja f ning artiklite 25 ja 32 nõuetele, on vastutava töötleja ülesanne igal juhul seda faktiliselt tõendada. Selline tõendamine peaks hõlmama alternatiivsete stsenaariumide kaalumist.

3.2 Kooskõla IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32

3.2.1 1. stsenaarium: registreeritud biomeetriline mall on ainult üksikisiku valduses, autentimise eesmärgil

34. Käesolevas jaos uuritakse, kas reisijate biomeetrilise malli säilitamine ainult üksikisiku valduses, näiteks tema ainukontrolli all[48] olevas isiklikus seadmes[49], autentimise eesmärgil[50], on kooskõlas IKÜM artikli 5 lõike 1 punktiga f ning artiklitega 25 ja 32 (edaspidi „esimene stsenaarium“). Selles jaos uuritakse ka 1. stsenaariumi asjakohaseid kaitsemeetmeid, võttes arvesse IKÜM artikleid 25 ja 32.

Stsenaariumi kirjeldus

35. 1. stsenaariumi puhul asub iga selliseks töötlemiseks nõusoleku andnud reisija registreeritud biomeetriline mall ainult üksikisiku valduses, näiteks iga reisija ainukontrolli all olevas isiklikus seadmes. Reisijad autenditakse (1:1 võrdlus), kui nad lennujaamas konkreetseid kontrollpunkte läbivad.

36. Registreerimine toimub lennujaama käitaja poolt kas kaugühenduse teel lennujaama käitaja rakenduse kaudu[51] või lennujaama terminalides, kus on tagatud asjakohane isikusamasuse tagamise

[45] Euroopa Andmekaitsenõukogu suunised 5/2020 määruse (EL) 2016/679 kohase nõusoleku kohta, punkt 5.
[46] Kohtuasi C-439/19: Latvijas Republikas Saeima, punktid 110 ja 113; Kohtuotsus, Euroopa Kohus (suurkoda), 4. juuli 2023, Meta *vs*. Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, punkt 108.
[47] Kohtuasi C-708/18: M5A-ScaraA, punktid 52–56, C-92/09 ja C-93/09: Volker und Schecke, punkt 87; C-439/19 Latvijas Republikas Saeima, punktid 98, 110 ja 113. Vt ka artikli 29 töörühma arvamus 3/2012 biomeetriliste tehnoloogiate kohta, lk 8.
[48] See ei piira vastutava töötleja üldist vastutust seoses töötlemisega.
[49] Alternatiivina võib üksikisik oma biomeetrilise malli välja printida ja säilitada seda paberil.
[50] Nagu on näitlikustatud taotluse I lisas esitatud 1. kasutusjuhtumis.
[51] Andmekaitsenõukogu märgib, et tulevikus võidakse ette näha alternatiivsed viisid selliseks registreerimiseks ja registreerimine võiks toimuda ilma konkreetse lennujaama käitaja rakenduseta, näiteks kasutaja digitaalse rahakoti kaudu.

usaldusväärsuse tase (nt asjakohane eIDASe usaldusväärsustase[52]). Registreerimine seisneb biomeetrilise malli ja töötlemiseks vajalike isikutuvastusandmete (edaspidi „**ID**“) salvestamises reisija seadmesse[53]. Registreerimine toimub ainult üks kord ja see kehtib konkreetse ajavahemiku jooksul (näiteks vastavalt reisija passi kehtivusajale). Lennujaama käitaja ei säilita reisija isikuandmeid ega biomeetrilisi andmeid pärast registreerimisprotsessi lõppu.

37. Reisija ID ja biomeetriline mall salvestatakse lokaalselt iga reisija seadmesse (nt lennujaama käitaja mobiilirakenduses või digitaalse rahakoti rakenduses). Seejärel saab seadet kasutada reisijate isikut tõendava dokumendi ja biomeetrilise malli edastamiseks või selle kohta päringute tegemiseks. Seade võib sisaldada lennuinfot ja/või pardakaarti. Näiteks krüpteeritakse see teave võtmega, mis on ainult lennujaama käitaja valduses – ehk kodeeritakse ruutkood, mida saab trükkida paberile või kuvada reisija seadme ekraanil. Sellisel juhul näitaks reisija seda ruutkoodi lennujaama spetsiaalsetele kontrollseadmetele, mis on varustatud ruutkoodi-skanneri ja kaameraga.

38. Turvalisuse tagamiseks krüpteeritakse ruutkoodid võrdlemise ajal võtmega, mis on lennujaama käitaja valduses kes on ainus, kes saab ruutkoodid dekrüpteerida. Reisijate biomeetrilisi andmeid säilitatakse ainult väga lühikese aja jooksul ja need kustutatakse pärast võrdlemise lõpuleviimist. Tuleb märkida, et säilitamisega seotud turvameetmed sõltuvad osaliselt reisija seadme turvalisusest.

Euroopa Andmekaitsenõukogu hinnang

39. 1. stsenaariumis kirjeldatakse tehnilisi ja korralduslikke meetmeid, mille eesmärk on tagada andmesubjektidele avalduvatele ohtudele vastav turvalisuse tase, nagu on nõutud IKÜM artikli 5 lõike 1 punktis f ja artiklis 32. Reisijad autenditakse (1:1 võrdlus), kui nad lennujaamas spetsiaalseid kontrollpunkte läbivad. Selle stsenaariumi puhul toimub peamine andmete võrdlemine kontrollitud keskkonnas[54], kus reisijad on aktiivselt kaasatud ja neil on suurem kontroll oma andmete üle. Eelkõige kontrollitakse ainult neid reisijaid, kes on selliseks töötlemiseks nõusoleku andnud, ning kuna neid kontrollitakse spetsiaalses keskkonnas, siis ei koguta biomeetrilisi andmeid teistelt reisijatelt, kes selliseks töötlemiseks nõusolekut ei ole andnud. Lisaks on nõusoleku andnud reisijatel võimalus töötlemine igal ajal peatada, kustutades andmed oma seadmest.

40. Näotuvastus, mis põhineb biomeetrilisel mallil, mida säilitatakse ainult üksikisiku valduses ja mis võib olla näiteks reisija ainukontrolli all olevas individuaalses seadmes, mida kasutatakse spetsiaalse liidese kaudu autentimiseks konkreetsetes kontrollpunktides, kujutab endast teatavatel tingimustel väiksemat ohtu võrreldes keskandmebaasis säilitatavate biomeetriliste andmete kasutamisega[55]. Selline lokaalne säilitamine koos asjakohaste kaitsemeetmetega[56] vähendab isikuandmetega seotud

[52] E-identimise ja e-tehingute jaoks vajalike usaldusteenuste raamistik (edaspidi „**eIDAS**“), mille aluseks on Euroopa Parlamendi ja nõukogu 11. aprilli 2024. aasta määrus (EL) 2024/1183, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega.

[53] Käesolevas arvamuses tähendavad isikuandmed selliseid andmeid nagu perekonnanimi, eesnimi, sünniaeg jne, mille õigsust on kontrollitud isikut tõendava dokumendist või passist.

[54] „Kontrollimatu keskkond“ – näotuvastuse kasutamine isikusamasuse tuvastamiseks ilma andmesubjektide aktiivse kaasamiseta, kus iga seirepiirkonda siseneva näo malli võrreldakse andmebaasis säilitatavate mallidega, mis on saadud laialt elanikkonna osalt, vt Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses, punkt 17.

[55] Euroopa Andmekaitsenõukogu suunised 5/2022 näotuvastuse kohta õiguskaitses, punkt 17.

[56] Nagu on selgitatud allpool punktis 46.

rikkumiste raskusastet võrreldes tsentraliseeritud säilitamisega, kus mõjutatud isikute arv on suurem, ning tagab, et juurdepääs biomeetrilisele mallile toimub andmesubjekti aktiivsel osalusel.

41. Lisaks võiks võrdlemine toimuda lennujaamas kohapeal, nii et võrreldakse näiteks ruutkoodis sisalduvat biomeetrilist malli mudeliga, mis on arvutatud kontrollseadme kaameraga salvestatud biomeetrilise malli põhjal. Konkreetset kontrolli teostav vastutav töötleja (kes võib olla lennujaama käitaja või lennufirma sõltuvalt sellest, kas seda tehakse lennujaama julgestuskontrollipunktides, pagasi äraandmisel, pardaleminekul ja/või reisijate *lounge*'ile juurdepääsul) avaldab ja kasutab ainult võrdlemise tulemust. Asjaolu, et võrdlemiseks vajaliku teabe (nt ruutkoodi) peab esitama üksikisik, on teine tegur,[57] mis suurendab autentimise turvalisust.

42. Pidades silmas kooskõla IKÜM artikliga 25 ja eelkõige selleks, et järgida võimalikult väheste andmete kogumise nõuet, tuleks tagada, et töötlemine vastab vajalikkuse põhimõttele. 1. stsenaariumi puhul võib valitud meetmeid pidada eesmärgi (st reisijatevoo sujuvamaks muutmise) seisukohalt vajalikkuse põhimõttele vastavaks, kui vastutav töötleja suudab töötlemise tingimustest lähtuvalt tõendada, et puuduvad vähem sekkuvad alternatiivsed lahendused, mis suudaksid sama eesmärki tõhusalt saavutada. Näiteks võib vastutav töötleja tõendada, et isegi kui reisijatel tuleks oma seadet näidata, kiirendab 1. stsenaarium kontrolliprotsessi võrreldes praeguse olukorraga, mille käigus inimene kontrollib, kas pardakaardil olev nimi on sama, mis reisija isikut tõendavas dokumendis[58]. Ilmselgelt ei saa seda aga tõendada, kui praegu reisijate isikusamasust nende ametliku isikut tõendava dokumendi alusel ei kontrollita (vt selle kohta eespool punkt 18).

43. Lisaks ei säilita lennujaama käitaja biomeetrilisi malle pärast registreerimist ja biomeetriliste andmete säilitamise aeg kontrolli läbi viiva vastutava töötleja poolt on väga lühike, sest sellised andmed kustutatakse kohe, kui võrdlemine on lõpule viidud. Seega näib, et 1. stsenaariumis valitud meetmete puhul on isikuandmete töötlemise ulatus ja säilitamistähtaeg piiratud.

44. Proportsionaalsuse põhimõtet järgides saab sellisest töötlemisest tulenevat isikuandmetesse sekkumist tasakaalustada reisijate aktiivse kaasamisega, kuna nende biomeetrilised andmed on ainult nende valduses. Lisaks, võttes arvesse eespool kirjeldatud meetmeid ja eeldades, et vastutav töötleja rakendab kõnealuse konkreetse töötlemise puhul nõutavaid piisavaid kaitsemeetmeid, võib asjakohaste meetmete rakendamine tagada ohule vastava turvalisuse taseme. Sellisel juhul võib negatiivset mõju andmesubjektide põhiõigustele ja -vabadustele pidada proportsionaalseks eeldatava kasuga.

45. Seetõttu järeldab andmekaitsenõukogu eeltoodut arvesse võttes vastuseks küsimusele 1.1, et sellist töötlemist võib pidada **IKÜM artikli 5 lõike 1 punktiga f ning artiklitega 25 ja 32 põhimõtteliselt kooskõlas olevaks, kui kohaldatakse asjakohaseid kaitsemeetmeid.**

Asjakohased kaitsemeetmed

46. Seda liiki juhtumi puhul leiab andmekaitsenõukogu vastuseks küsimusele 1.2, et tuleks rakendada vähemalt järgmisi kaitsemeetmeid. *Muid kaitsemeetmeid kui neid mis on käesolevas arvamuses kirjeldatud, võib kasutada samade turvalisuse ja andmekaitse eesmärkide saavutamiseks ning need võivad olla seaduslikud, kui need tagavad vastavuse kohaldatavale õigusraamistikule.*

[57] Näiteks leevendab see identiteedi võltsimise ohtu. Vt ka kaitsemeede C.1.2 allpool.
[58] Võib ka väita, et biomeetriline kontroll võib olla vähem veaohtlik kui inimese poolt tehtav kontroll.

47. Märkus: *tegemist on kõrgetasemelise ja mittetäieliku ülevaatega võimalikest asjakohastest kaitsemeetmetest, mida vastutav töötleja võiks rakendada 1. stsenaariumiga sarnase lahenduse korral. Nende asjakohasust tuleb analüüsida juhtumipõhiselt lähtuvalt IKÜM artiklitest 25 ja 32. Kõik vastutavad töötlejad peavad tagama, et nad teevad ise oma andmekaitsealase mõjuhinnangu[59] ja arvestama, et nende konkreetsed lahendused võivad vajada täiendavaid meetmeid, mida käesolevas arvamuses ei käsitleta.*

A. Üldine teave

A.1 Andmetöötluse mõju hindamine

A.1.1 Teha kooskõlas IKÜM artikli 35 nõuetega andmekaitsealane mõjuhinnang, kui vastutav töötleja kavandab uut töötlemistoimingut, millega tõenäoliselt kaasneb suur oht. See on 1. stsenaariumi puhul tõenäoline, kuna stsenaarium hõlmab biomeetriliste andmete ulatuslikku töötlemist[60]. Hinnata näotuvastussüsteemi rakendamise asjakohasust, sealhulgas selle vajalikkust ja proportsionaalsust taotletavate eesmärkide suhtes[61], projekteerimise varases etapis ja kogu tootearenduse olelusringi jooksul;

A.1.2 Konsulteerida asjaomase järelevalveasutusega, kui töötlemise tulemusena tekiks hoolimata vastutava töötleja poolt ohu leevendamiseks võetavatest meetmetest ikka suur oht[62].

A.2 Andmesubjekti õigused ja kaitsemeetmed, mida vastutavad töötlejad saavad rakendada

A.2.1 Kaitsemeetmed valenegatiivsete juhtumite käsitlemiseks. Leevendada vanuselise, soolise ja rassilise kallutatuse riski, „hinnates korrapäraselt, kas algoritmid toimivad kooskõlas eesmärkidega, ning kohandades algoritme, et leevendada kallutatust, mida pole veel käsitletud, ja tagada töötlemise õiglus“[63]. Näiteks rakendades inimjärelevalvet ja -sekkumist, et leevendada mis tahes kallutatust ja tagada, et reisijaid ei häbimärgistata ega profileerita;

A.2.2 Tagada, et igasugune isikuandmete töötlemine on läbipaistev ning üksikisikud on teadlikud ja saavad kontrollida, kuidas nende andmeid iga töötlemistoimingu puhul töödeldakse[64];

---

[59] Isikuandmete kaitse üldmääruse artikkel 35.
[60] Isikuandmete kaitse üldmääruse artikli 35 lõige 3 ja 13. oktoobril 2017 vastu võetud artikli 29 töörühma suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ määruse (EL) 2016/679 tähenduses (WP 248 rev. 01), mille on heaks kiitnud Euroopa Andmekaitsenõukogu.
[61] Isikuandmete kaitse määruse artikli 35 lõike 7 punkt b.
[62] Isikuandmete kaitse üldmääruse artikli 36 punkt 1.
[63] Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, joonealune märkus 60, punkt 70.
[64] Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, punkt 68 ja isikuandmete kaitse üldmääruse põhjendus 7.

A.2.3 Tagada, et on kehtestatud meetmed eesmärgi piirangu põhimõtte järgimiseks, et andmeid ei kasutataks muudel eesmärkidel, näiteks julgeoleku või koolituse eesmärgil;

A.2.4 Tagada asjakohaste meetmetega (näiteks kasutades piisavat teravussügavust ja jäädvustamisala, et vältida teiste taustal olevate või ümbritsevate reisijate pildistamist või eraldades spetsiaalselt järjekordi, mis on näotuvastuse jaoks selgelt märgistatud), et isikust, kes ei ole näotuvastusega nõus ei salvestata fotot ega videot.

A.2.5 Kui näotuvastusega nõustunud ja mittenõustunud reisijate jaoks kasutatakse samu kontrollseadmeid või kui reisijad, kes näotuvastusega ei nõustunud, võivad vaateväljale ilmuda ajal, mil süsteemi ei kasutata, tuleb enne foto või video salvestamise alustamist oodata nõusoleku andnud reisija kinnitavat märguannet;

A.2.6 Andmesubjekti võimalus igal ajal kustutada üksnes tema käes olevaid andmeid (biomeetriline mall[65]), mida hoitakse mobiilirakenduses või digitaalses rahakotis[66];

A.2.7 Võimalike alternatiivide või varulahenduste pakkumine (st reisijatele, kes ei nõustu oma biomeetriliste andmete kasutamisega, reisijatele, kes ei saa selliseid lahendusi kasutada, või reisijatele, kelle andmed ekslikult tagasi lükatakse), et tagada ka see, et reisijad, kes ei nõustu oma biomeetriliste andmete kasutamisega, ei kannataks kahjulike tagajärgi[67];

A.2.8 Kui kasutatakse rakendusi, peaksid need olema hoolikalt kavandatud ja konfigureeritud, et mitte koguda mittevajalike andmeid ja vältida kolmandate isikute tarkvaraarenduskomplektide kasutamist, mis koguvad andmeid muudel eesmärkidel.

A.3 Aruandlus

A.3.1 Hinnata, kas on olemas asjakohased toimimisjuhendid või sertifitseerimismehhanismid, mis aitavad tõendada IKÜM artiklis 32 sätestatud töötlemise turvalisust[68]. Kontrollida, kas meetmed on konkreetse töötlemise puhul asjakohased. Asjakohaste meetmete kindlaksmääramisel võivad abiks olla standardid[69], parimad tavad ja toimimisjuhendid, mida tunnustavad vastutavate töötlejate erinevaid kategooriaid esindavad ühendused ja muud organid;

A.3.2 Tagada kasutaja seadme elementaarne turvakontroll enne registreerimisetappi, võttes arvesse, et reisija vastutab ise ka oma andmete kaitse eest, kuna need on salvestatud tema

[65] 1. stsenaariumi kaitsemeetmetes sisalduvad viited biomeetrilisele mallile vastavad 2. stsenaariumis esitatud võtme/saladuse viidetele.
[66] See kaitsemeede kehtib ainult 1. stsenaariumi puhul.
[67] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 86.
[68] Isikuandmete kaitse üldmääruse artikli 32 punkt 3 ja Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, punkt 10.
[69] Vt näiteks ISO/IEC 2382-37.

seadmesse. Selliste tehniliste kontrollide näited on esitatud allpool jaotises C.2 „Taristu ja võrk“.

B. Korralduslikud meetmed:

B.1 Põhimõtted ja vastavus

B.1.1. Tagada, et kehtestatud on sisemised juurdepääsukontrollid[70] koos eeskirjadega administraatoritele;

B.1.2 Kui näotuvastusteenust võib osutada üks andmete töötlemises osalev isik, ilma et teised asjaomased isikud peaksid isiku- või biomeetriliste andmete või mõlemaga kokku puutuma, tuleb keelata andmete edastamise nende teiste isikute kaudu. Näiteks ei pea lennufirma biomeetrilistele andmetele tehniliselt juurde pääsema, kui kasutatakse lennujaama ühist taristut, isegi kui see lennufirma tegutseb IKÜMi kohase töötlemise vastutava töötlejana;

B.1.3 Määrata kindlaks krüpteerimise ja võtme haldamise põhimõtted[71], mida on vaja näiteks isiku- ja biomeetriliste andmete töötlemiseks;

B.1.4 Tagada IKÜMi V. peatüki järgimist. Näiteks tagada nõuetele vastav edastamine, kui vastutav töötleja kasutab registreerimisprotsessi käigus kaugteenust, mille pakkuja asukoht on kolmandas riigis;

B.1.5 Kui kasutatakse volitatud töötlejaid, tuleb tagada, et on olemas volitatud töötleja leping kooskõlas IKÜM artikli 28 lõikega 3[72];

B.1.6 Tagada, et on kehtestatud menetlused inimjärelevalve ja -sekkumise juhtimiseks, eelkõige eksliku tagasilükkamise ja tehniliste või kasutatavusega seotud probleemide lahendamiseks.

B.2 Väljaõpe ja testimine

B.2.1. Tagada, et personal on saanud vastava väljaõppe;

B.2.2 Rakendada „tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise kord isikuandmete töötlemise turvalisuse tagamiseks[73];

[70] Euroopa Andmekaitsenõukogu suunised 04/2020 asukohaandmete ja kontaktide jälgimise vahendite kasutamise kohta COVID-19 puhangu kontekstis, vastu võetud 21. aprillil 2020 (edaspidi „**Euroopa Andmekaitsenõukogu suunised 4/2020 asukohaandmete ja kontaktide jälgimise vahendite kohta**“), SEC-10, lk 16.
[71] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 89.
[72] Isikuandmete kaitse üldmääruse artikli 28 lõige 3.
[73] Isikuandmete kaitse direktiivi artikli 32 lõike 1 punkt d.

B.2.3. Võtta kasutusele protsess, millega tagatakse, et reisija biomeetrilise malli[74] töötlemine autentimiseks on tehniliselt tõhus ja piisavalt täpne;

B.2.4. Tagada, et nii registreerimisel kui ka kontrollpunktis kogutud biomeetrilised mallid on usaldusväärseks biomeetriliseks töötlemiseks piisavalt kvaliteetsed.

C. Tehnilised meetmed:

C.1 Juurdepääs

C.1.1 Rakendada registreerimisetapis kaitsemeetmeid, et tagada *bootstrap*-meetodit järgiv registreerimisprotsess kontrollitud identiteediga. Näiteks, et tõhustada kasutajate identiteedi mitmikautentimise hindamist, võib kasutusele võtta erinevaid meetmeid alates salasõnaga kaitstud ühekordsetest linkidest rakenduse aktiveerimiseks kuni kohalike seadmete blokeerimise mehhanismideni;

C.1.2 Rakendada kaitsemeetmeid valepositiivsete juhtumite ja teise isikuna esinemise juhtumite käsitlemiseks ning ennetada pettusi[75];

C.1.3 Keelata väline juurdepääs isikutuvastus- ja biomeetrilistele andmetele[76];

C.1.4 Tagada, et andmete töötlemine registreerimise, edastamise ja võrdlemise etapis toimub kohapeal. Võrdluskoht peaks olema isiku seadmele võimalikult lähedal. Malli võrdlemise võimaldamine konkreetses seadmes võib vajada suhtlust väljaspool lennujaama asuvate teenuseosutajatega, mis hõlmab avalike võrkude kasutamist, mille puuduseks on mõju juurdepääsetavusele ja malli edastamine välistele üksustele;

C.1.5 Autentida kasutaja uue lennu lisamiseks ja uue krüpteeritud ruutkoodi genereerimiseks;

C.1.6 Rakendada meetmeid, et ei tekiks olukorda, kus reisija võib kaotada juurdepääsu oma ruutkoodile.

C.2 Taristu ja võrk

C.2.1 Ajakohased operatsioonisüsteemi tingimused ja autentimine, mis võimaldab rakenduse/digitaalse rahakoti toimimiseks seadmele juurde pääseda, sealhulgas isiku- ja biomeetriliste andmete automaatne kustutamine, kui operatsioonisüsteem on aegunud ja ohustab turvalisust;

[74] 1. stsenaariumi kaitsemeetmetes sisalduvad viited biomeetrilisele mallile vastavad 2. stsenaariumis esitatud võtme/saladuse viidetele.

[75] 2022. aasta jaanuaris avaldatud digiidentiteeti käsitlev ENISA aruanne suveräänidentiteedi põhimõtte edendamise kohta (ENISA Report on Digital Identity on leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust).

[76] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 89.

C.2.2 Võrdlemisseadmete (st kontrollseadmete) eraldamine võrgust kasutamise ajal ja muude turvalisuse tagamiseks vajalike meetmete võtmine;

C.2.3 Biomeetrilise võrdlustoimingu sooritamine (servtöötlus) reisija seadmes või kontrollseadmes;

C.2.4 Lahendused reisijate individuaalsete seadmete turvanõrkuste kõrvaldamiseks, sealhulgas (vähemalt) biomeetriliste ja isikuandmete krüpteerimine puhkeolekus;

C.2.5 Kasutada (vähemalt) biomeetriliste andmete säilitamiseks üksnes kasutaja valduses olevaid turvalisi meetodeid[77], näiteks kasutades nutitelefonis turvalist enklaavi;

C.2.6 Turvameetmete rakendamine, et tagada ruumide, sealhulgas lennujaama biomeetrilise töötlemise terminali füüsiline turvalisus. Isikuandmete töötlemissüsteemi elementide (nt arvutamine, andmevoog, ajutine või pikaajaline säilitamine) ja biomeetriliste andmete turvalisuse kõrge taseme tagamine.

C.3 Andmeturve ja andmete haldamine kasutaja identiteedi kontrollimisel

C.3.1 Andmete eraldamine edastamise ja säilitamise ajal vähemalt kolme eri rühma, näiteks: isikutuvastusandmed, biomeetrilised andmed ja lennuandmed[78]. Tagamine, et andmed on edastamise ja säilitamise vahel nõuetekohaselt krüpteeritud;

C.3.2 Kehtestada tehnilised meetmed, millega tagatakse, et kontrollpunktides töödeldakse ja kontrollitakse ainult neid andmeid, mida võib nendes konkreetsetes kontrollpunktides õiguspäraselt töödelda;

C.3.3 Tagada andmete tõhusa kustutamise turvalise menetluse kaudu[79] (nt põhimälu, vahemälu, võimalike varukoopiate kustutamine) ja hinnata, millal peaks andmete kustutamine olema automaatne. Andmete säilitamise aeg tuleks kehtestada rangelt automaatsete menetluste abil, ilma et üksikisikul oleks vaja võtta täiendavaid meetmeid[80];

C.3.4 Tagada andmete autentsus ja terviklus (näiteks allkiri)[81];

C.3.5 Reisijate biomeetrilisi andmeid säilitatakse registreerimispunktis ja kontrollpunktis ainult väga lühikeseks ajaks ning kustutatakse niipea, kui reisija on kontrollpunkti läbinud;

[77] 1. stsenaariumi kaitsemeetmetes sisalduvad viited biomeetrilisele mallile vastavad 2. stsenaariumis esitatud võtme/saladuse viidetele.
[78] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 89.
[79] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 89.
[80] Euroopa Andmekaitsenõukogu „Artiklit 25 käsitlevad suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse“, punkt 82.
[81] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 89.

C.3.6 Kui registreerimiseks kasutatakse rakendust, tuleb rakenduse väljatöötamise ajal kohaldada mobiilirakenduste turvastandardeid ning kolmanda isiku poolt tehtud turvakontrolle;

C.3.7 Tagada, et lennujaamas on registreerimise etapis kehtestatud turvameetmed, et säilitada reisija biomeetriliste andmete konfidentsiaalsus ja terviklus. Näiteks kui ruutkood trükitakse kioskis, ei tohiks ruutkoodi kioskis kuvada, et kuritahtlikud isikud ei saaks pilti teha. Lühikese raadiusega edastuse korral peaks edastamine toimuma kasutaja aktiivsel osalemisel ja lähedust tagava kanali kaudu;

C.3.8 Ainult üksikisiku valduses olevaid andmeid[82] tuleks säilitada turvaliselt isiku seadmes ning kõik seadme operatsioonisüsteemidega seotud võimalikke nõrkusi tuleb kontrollida asjakohastes turbepaikades. Trükitud ruutkoodi puhul tuleks üksikisikut teavitada, et selles sisalduvad andmed on eriti tundlikud ja sellest, mida nendega on võimalik teha;

C.3.9 Tagada, et registreerimisel järgitakse piisavaid kaugtuvastamise mehhanisme[83].

3.2.2 2. stsenaarium: registreeritud biomeetrilise malli tsentraliseeritud säilitamine lennujaamas krüpteeritud kujul kus võti/saladus on üksnes reisija valduses, autentimise eesmärgil

48. Käesolevas jaos uuritakse, kas reisijate registreeritud biomeetriliste mallide tsentraliseeritud säilitamine keskses andmebaasis, krüpteeritud kujul ja üksnes reisija valduses oleva võtme/saladusega[84] on kooskõlas IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32 (edaspidi „**2. stsenaarium**“). Selles jaos uuritakse ka 2. stsenaariumi asjakohaseid kaitsemeetmeid, võttes arvesse IKÜM artikleid 25 ja 32.

Stsenaariumi kirjeldus

49. 2. stsenaariumi puhul toimub registreerimine ainult üks kord konkreetse kehtivusaja jooksul (näiteks üks aasta pärast viimast lendu, kuni passi kehtivusaja lõpuni), kas kaugmeetodil asjakohasel usaldusväärsel isikusamasuse tagamise tasemel (nt eIDASe asjakohane usaldusväärsuse tase) või lennujaama terminalides. Registreerimist kontrollib lennujaama käitaja ning selle käigus genereeritakse isiku- ja biomeetrilised andmed, mis on võtmega/saladusega krüpteeritud.

50. Andmebaas asub lennujaama ruumides lennujaama käitaja kontrolli all. Konkreetse üksikisiku krüpteerimisvõtmeid/saladusi hoitakse üksnes selle isiku seadmes (näiteks lennujaama käitaja mobiilirakenduses). Rakendus võib genereerida ruutkoodi, mis sisaldab võtit/saladust, mille võib välja

[82] 1. stsenaariumi kaitsemeetmetes sisalduvad viited biomeetrilisele mallile vastavad 2. stsenaariumis esitatud võtme/saladuse viidetele.
[83] Vt ENISA aruanne *Report on Remote ID Proofing: Analysis of methods to carry out identity proofing remotely* (aruanne identiteedi kaugtuvastamise kohta: identiteedi kaugtuvastamise meetodite analüüs), märts 2021.
[84] Nagu on näitlikustatud taotluse I lisas esitatud kasutusjuhtumis 2.

trükkida või kuvada seadme ekraanil[85]. Lisaks kasutab lennujaama käitaja teist krüpteerimiskihti[86], mille võtmed on lennujaama käitaja kontrolli all.

51. Reisijad autenditakse (1:1 võrdlus), kui nad lennujaamas konkreetseid kontrollpunkte läbivad. Reisijad, kes otsustavad läbida biomeetrilised kontrollpunktid, näitavad oma ruutkoodi spetsiaalsele kontrollseadmele, mis on varustatud ruutkoodi skanneri ja kaameraga. Reisija indeks saadetakse andmebaasi, et taotleda krüpteeritud malli, mis laaditakse alla ja mida kontrollitakse kohapealses seadmes ja/või kasutaja seadmes. Kontrollpunkti töötaja näeb ja kasutab ainult võrdlemistoimingu tulemust[87].

52. Selles stsenaariumis ei edastata lennujaamade vahel isiku- ja biomeetrilisi andmeid ning keskandmebaasid ei ole omavahel ühendatud ega koostalitlusvõimelised.

Euroopa Andmekaitsenõukogu hinnang

53. 2. stsenaariumi puhul säilitatakse reisijate registreeritud biomeetrilisi malle tsentraliseeritult, kuid krüpteeritud kujul, ja võti/saladus on üksnes reisija valduses. 2. stsenaariumi puhul toimub reisijate autentimine (1:1 võrdlus).

54. Selle stsenaariumi puhul tehakse ettepanek saavutada reisijatevoo sujuvamaks muutmine (st kontrollide kiirendamine) tsentraliseeritud süsteemi kasutamisega. Euroopa Andmekaitsenõukogu on varem märkinud, et sellist lahendust võib pidada toimivaks alternatiiviks registreeritud biomeetriliste mallide detsentraliseeritud säilitamisele[88] (mida on kirjeldatud 1. stsenaariumis), kui selleks on objektiivsed vajadused ja kasutatakse asjakohaseid kaitsemeetmeid (vt allpool punktis 60 kirjeldatud kaitsemeetmed).

55. Turvakaalutlustel on iga isiku andmed krüpteeritud konkreetse võtmega, mis on üksnes üksikisiku valduses ja tema ainukontrolli all.Asjaolu, et võrdlemiseks vajaliku teabe (nt saladuse/võtme) peab esitama üksikisik on teine samm ja see suurendab autentimise turvalisust.[89] Lisaks lisab lennujaama käitaja teise krüpteerimiskihi, mille võtmed on lennujaama käitaja kontrolli all. 2. stsenaariumis saadetakse isiku indeks isikuga seotud biomeetriliste andmete saamiseks keskandmebaasi. Seejärel saadetakse need andmed (krüpteerituna) kontrollpunktis asuvasse arvutisse, kus need võrdlustoimingu tegemiseks dekrüpteeritakse, ning kontrollpunkti töötaja näeb ja kasutab ainult võrdlustoimingu tulemust. Kui isiku võtit/saladust hoitakse kontrollpunktis asuvas arvutis ja keskandmebaasi saadetakse krüpteeritud biomeetrilise malli saamiseks ainult reisija indeks, võib selliseid turvameetmeid seega pidada IKÜM artikli 5 lõike 1 punktiga f ja artikliga 32 kooskõlas olevaks.

56. Pidades silmas kooskõla IKÜM artikliga 25 ja eelkõige selleks, et järgida võimalikult väheste andmete kogumise nõuet, tuleks tagada, et töötlemine vastab vajalikkuse põhimõttele. 2. stsenaariumi puhul võib valitud meetmeid pidada eesmärgi (st lennujaamades reisijatevoo sujuvamaks muutmise)

[85] Prantsusmaa järelevalveasutus on täiendavalt selgitanud, et nõutava teabe saatmiseks võib olla ka muid tehnilisi lahendusi, näiteks lähitoimeside protokoll.
[86] Võti/saladus (üksikisiku valduses) on omakorda krüpteeritud lennujaama käitajale kuuluva teise võtmega.
[87] Prantsusmaa järelevalveasutus selgitas, et see säilitamistähtaeg on näitlik ja seda võib pidada vastuvõetavaks, arvestades, et võti asub üksikisiku valduses ja selle võib valida registreerimise etapis. Tuleb siiski märkida, et sellist säilitamistähtaega võib kohandada.
[88] Euroopa Andmekaitsenõukogu suunised 3/2019 videoseadmete kohta, punkt 88.
[89] Näiteks leevendab see identiteedi võltsimise ohtu. Vt ka kaitsemeede C.1.2.

seisukohalt vajalikkuse põhimõttele vastavaks, kui vastutav töötleja suudab töötlemise tingimustest lähtuvalt tõendada, et puuduvad vähem sekkuvad alternatiivsed lahendused, mis suudaksid sama eesmärki tõhusalt saavutada. 2. stsenaariumi puhul tuleks reisijatel ikkagi seadet näidata[90]. Siiski võib vastutav töötleja tõendada, et 2. stsenaarium kiirendab kontrolliprotsessi võrreldes praeguse olukorraga, mille käigus inimene kontrollib, kas pardakaardil olev nimi on sama, mis reisija isikut tõendavale dokumendis[91], või võrreldes 1. stsenaariumiga. Ilmselgelt ei saa seda aga tõendada, kui praegu reisijate isikusamasust nende ametliku isikut tõendava dokumendi alusel ei kontrollita (vt selle kohta eespool punkt 18).

57. Proportsionaalsuse põhimõtet järgides saab sellisest töötlemisest tulenevat sekkuvust tasakaalustada reisija aktiivse kaasamisega, kelle ainukontrolli all on nende krüpteeritud andmete võti/salasõna. Lisaks näib, et turvariske, mis kaasnevad reisijate biomeetriliste andmete säilitamisega keskandmebaasis, kui võti on üksnes reisijate valduses, saab leevendada asjakohaste kaitsemeetmete kasutamisega (vt allpool punktis 60 käsitletud kaitsemeetmeid). Eeldades, et vastutav töötleja rakendab konkreetse töötlemistoimingu puhul nõutavaid asjakohaseid kaitsemeetmeid, saaks ta seega leevendada keskse andmebaasi kasutamisest tulenevaid turvariske ning negatiivset mõju andmesubjektide põhiõigustele ja -vabadustele ning seda võiks pidada proportsionaalseks eeldatava kasuga. Loomulikult tuleks kõikidel juhtudel tagada, et töödeldakse ainult eesmärgi seisukohalt vajalikke andmeid ja kontrollitakse ainult nõusoleku andnud reisijaid. Sellega puuduks oht, et kogutakse biomeetrilisi andmeid teiste reisijate kohta, kes ei ole nõusolekut andnud.

58. Taotluses on näitena märgitud, et 2. stsenaariumi puhul võib krüpteeritud andmete andmebaasis säilitamise aeg olla tavaliselt üks aasta pärast üksikisiku viimast lendu ja kuni passi kehtivusaja lõpuni. Taotluses ei ole esitatud teavet, mis objektiivselt põhjendaks seda pikka ajavahemikku, kuigi võib eeldada, et selline säilitamistähtaeg on kavandatud mugavuse eesmärgil, pidades silmas tulevasi lende. Selleks et saavutada selle stsenaariumi puhul säilitamistähtaja osas kooskõla IKÜM artikli 5 lõike 1 punktiga e, peaksid vastutavad töötlejad suutma põhjendada, miks selline säilitamistähtaeg on konkreetsetel juhtudel eesmärgi saavutamiseks vajalik. Andmekaitsenõukogu soovitab vastutavatel töötlejatel näha ette võimalikult lühike säilitamistähtaeg, võttes arvesse ka reisijaid, kes lendavad väga harva, ning pakkuda andmesubjektidele võimalust määrata neile sobiv säilitamistähtaeg.

59. Neid kaalutlusi arvesse võttes järeldab andmekaitsenõukogu vastuses küsimusele 2.1.1, et sellist töötlemist võib pidada **IKÜM artikli 5 lõike 1 punktiga e, artikli 5 lõike 1 punktiga f ning artiklitega 25 ja 32 põhimõtteliselt kooskõlas olevaks, kui kohaldatakse asjakohaseid kaitsemeetmeid.**

Asjakohased kaitsemeetmed

60. Seda liiki stsenaariumi puhul leiab andmekaitsenõukogu vastuseks küsimusele 2.1.2, et **lisaks 1. stsenaariumis loetletud kaitsemeetmetele** tuleks rakendada vähemalt järgmisi kaitsemeetmeid. *Muid kui käesolevas arvamuses kirjeldatud kaitsemeetmeid võiks kasutada samade turvalisuse ja andmekaitse eesmärkide saavutamiseks ning need võivad olla seaduslikud, kui need tagavad vastavuse kohaldatavatele õigusraamistikele.*

[90] Prantsusmaa järelevalveasutus on täiendavalt selgitanud, et malli esitamiseks võib olla ka muid võimalusi, nt võib see olla paberile trükitud. Samuti on Euroopa Andmekaitsenõukogu nõus, et tulevikus võiks ette näha alternatiivse, nt lähiväljasidesüsteemil põhineva tehnoloogia kasutamise.

[91] Võib ka väita, et biomeetriline kontroll võib olla vähem veaohtlik kui inimese poolt tehtav kontroll.

61. Märkus: *tegemist on kõrgetasemelise ja mittetäieliku ülevaatega võimalikest asjakohastest kaitsemeetmetest, mida vastutav töötleja võiks rakendada 2. stsenaariumiga sarnase lahenduse korral. Nende sobivust tuleb analüüsida juhtumipõhiselt lähtuvalt IKÜM artiklitest 25 ja 32. Kõik vastutavad töötlejad peavad tagama, et nad teevad ise oma andmekaitsealase mõjuhinnangu ja arvestama, et nende konkreetsed lahendused võivad vajada täiendavaid meetmeid, mida käesolevas arvamuses ei käsitleta.*

D. Üldteave

D.1 Andmesubjekti õigused ja kaitsemeetmed, mida vastutavad töötlejad saavad rakendada

D.1.1 Tagada, et reisijal on kontroll kõigi oma andmete säilitamistähtaja üle. Säilitamistähtaeg peaks piirduma konkreetse eesmärgi saavutamiseks vajalikuga. Maksimaalse ajavahemiku kehtestamise aluseks peaks olema erinevate tegurite põhjalik analüüs, näiteks isikut tõendava dokumendi kehtivus. Andmesubjektidele tuleks pakkuda võimalust määrata kindlaks säilitamistähtaeg, mida nad eelistavad ja mis võib olla lühem kui tavapärane säilitamistähtaeg;

D.1.2 Andmesubjekti võimalus igal ajal taotleda selliste andmete kustutamist, mis on üksnes tema valduses (võti/saladus) ja mida hoitakse mobiilirakenduses või digitaalses rahakotis[92];

D.1.3 Tagada, et keskserveri asukoht võimaldab pädevatel järelevalveasutustel teha tõhusat järelevalvet.

E. Korralduslikud meetmed:

E.1 Põhimõtted ja vastavus

E.1.1 Usaldus keskserveri vastu peab olema piiratud. Tagada, et keskserveri haldajad järgivad selgelt määratletud eeskirju ja rakendavad kõiki vajalikke meetmeid serveri turvalisuse tagamiseks[93].

F. Tehnilised meetmed:

F.1 Juurdepääs

F.1.1 Pidada logisid selle kohta, kellel on juurdepääs isikuandmetele, eelkõige isikutuvastus- ja biomeetrilistele andmetele, ning millal toimus andmetele juurdepääs;

F.2 Taristu ja võrk

[92] See kaitsemeede kehtib ainult 2. stsenaariumi puhul.
[93] Euroopa Andmekaitsenõukogu suunised 4/2020 asukohaandmete ja kontaktide jälgimise vahendite kohta, PRIV-5, lk 17.

F.2.1 Tagada keskandmebaasi asjakohane turvalisus, sealhulgas kaitse käideldavusrünnete eest;

F.2.2 Tagada, et puudub internetiühendus keskandmebaasi, registreerimisseadmete ja võrdlusüksustega. Süsteemide käitamine ja hooldamine (nt varukoopiate tegemine, parandamine, seire jne) peab toimuma lennujaama ruumides kohapeal.

F.3 Andmeturve ja -haldus

F.3.1 Rakendada tipptasemel krüptograafilisi tehnikaid, et tagada rakenduse ja keskserveri vaheline teabevahetus[94];

F.3.2 Säilitada individuaalseid võtmeid/saladusi tasandil, kus neid dekrüpteerimiseks kasutatakse (st kontrollseadmes), ja kasutada indeksit ainult selleks, et saada keskandmebaasist tagasi vastav registreeritud biomeetriline mall;

F.3.3 Tagada, et võtme/saladuse vahetus kasutajaseadme ja kontrollseadme vahel oleks kaitstud võimaliku pealtkuulamise või kolmandatele isikutele edastamise eest;

F.3.4 Indekseerida keskandmebaasis säilitatav biomeetriline mall, et võimaldada 1:1 autentimist ning tagada, et see oleks kordumatu ja üksikisikuga seotud. Tagada, et indeks ei paljastaks reisija isikuandmeid ega oleks korrelatsioonis krüpteerimisvõtmega;

F.3.5 Asjakohaselt autentida ja krüpteerida keskandmebaasi ja kontrollpunktide vaheline andmeedastus ning tagada selleks isoleeritud võrgud;

F.3.6 Vältida kahesuunalisi ühendusi andmekogumite vahel (isiku- ja biomeetrilised andmed ning lennuandmed) ning säilitada andmebaasis ainult asjakohaseid ühesuunalisi linke. Näiteks ainult ühesuunalised lingid indeksist isikutuvastusandmeteni, indeksist krüpteeritud biomeetriliste andmeteni ja indeksist lennuandmeteni;

F.3.7 Tagada talitluspidevuse kord, näiteks asjakohaste tagavarasüsteemide olemasolu;

F.3.8 Tagada, et kontrollseadmes ei säilitata logisid krüpteeritud või krüpteerimata mallide kohta.

3.2.3 Registreeritud biomeetriliste isikutuvastusmallide tsentraliseeritud säilitamine

[94] Euroopa Andmekaitsenõukogu suunised 4/2020 asukohaandmete ja kontaktide jälgimise vahendite kohta, SEC-4, lk 16: „Näiteks võib kasutada järgmisi tehnikaid: sümmeetrilist ja asümmeetrilist krüpteerimist, räsifunktsioone, privaatse liikmesuse testi (private membership test), hulkade ühisosa leidmist (private set intersection), Bloomi filtreid, teabe privaatset hankimist (private information retrieval), homomorfset krüpteerimist“.

62. Käesolevas jaos uuritakse, kas reisijate registreeritud biomeetriliste mallide tsentraliseeritud säilitamine tuvastamise eesmärgil keskses andmebaasis, kui mallid ei ole üksnes reisija valduses oleva võtme/saladusega krüpteeritud, on kooskõlas IKÜM artikli 5 lõike 1 punktidega e ja f ning artiklitega 25 ja 32: 1) kui selliseid malle säilitatakse lennujaama käitaja kontrolli all olevas lennujaama andmebaasis[95] (edaspidi „**stsenaarium 3.1**“) ja 2) kui selliseid malle säilitatakse pilves lennufirma kontrolli all[96] (edaspidi „**stsenaarium 3.2**“).

63. Andmekaitsenõukogu leiab, et biomeetriliste andmete kasutamine **tuvastamise** eesmärgil suurtes keskandmebaasides rikub andmesubjektide põhiõigusi ja võib tuua andmesubjektidele kaasa tõsiseid tagajärgi[97]. Lisaks tuleks biomeetriliste andmete kasutamist uurida ka seoses nende töötlemise eesmärgiga, pidades silmas vajalikkuse ja proportsionaalsuse põhimõtteid[98].

3.2.3.1 Stsenaarium 3.1: tsentraliseeritud säilitamine lennujaamas asuvas andmebaasis lennujaama käitaja kontrolli all

Stsenaariumi kirjeldus

64. Stsenaariumi 3.1 puhul säilitatakse reisija registreeritud biomeetrilist malli lennujaama ruumides asuvas keskandmebaasis ja lennujaama käitaja kontrolli all krüpteeritud kujul. Eelkõige on reisijate andmed jagatud osadeks, mis tähendab, et nende isikutuvastusandmeid, registreeritud biomeetrilist malli ja lennuteavet säilitatakse kolmes erinevas andmebaasis. Sellised andmed krüpteeritakse erinevate võtmetega nii salvestamise ajal kui ka siis, kui need edastatakse võrdlemiseks serveritesse, kus lennujaama käitaja need seejärel dekrüpteerib.

65. Reisijad peavad igale lennule registreeruma lühikese aja jooksul enne väljumist (nt 48 tunni jooksul). Selline registreerimine võib toimuda kas kaugühenduse teel või lennujaama terminalides asjakohasel tasemel, mis tagab isikusamasuse usaldusväärsuse (nt eIDASe asjakohane usaldusväärsuse tase). Teise võimalusena võib registreerimine toimuda samas vormis, nagu on kirjeldatud 1. stsenaariumis, millisel juhul peavad reisijad edastama oma andmed oma digitaalsetest rahakottidest lennujaamasüsteemi 48 tunni jooksul enne väljumist.

66. Ka selle stsenaariumi korral näitavad reisijad end kaameraga varustatud spetsiaalse kontrollseadme ees. Seejärel saadetakse nende biomeetriline mall lennujaama keskserverisse, mis püüab võrrelda andmeid biomeetrilise keskandmebaasi andmetega. Seega on võimalik reisija tuvastada ja kontrollida, kas ta on tõepoolest väljuvale lennule (või pardalemineku kontrolli korral lennule, mille pardale minek parajasti toimub) registreeritud. Sõltuvalt kontrollpunktist võib päringu esitanud kontrollpunkti vastutavale töötlejale tagasi saadetud andmeid minimeerida, piirdudes näiteks „jah/ei“ vastuse või vajaduse korral võrdlustulemusega. Sellisel juhul edastatakse kontrollpunkti vastutavale töötlejale ainult päringu tulemus ja ainult seda ta kasutabki.

67. Eelkõige kasutatakse selle stsenaariumi puhul reisijate tuvastamist (1:N võrdlus), kus N on lennujaamas mitme päeva jooksul eeldatav reisijate arv. Lisaks toimub biomeetriline võrdlemine

[95] Nagu on näitlikustatud taotluse I lisas esitatud kasutusjuhtumis 3A.
[96] Nagu on näitlikustatud taotluse I lisas esitatud kasutusjuhtumis 3B.
[97] Vt näiteks ka artikli 29 töörühma arvamus 3/2012 biomeetriliste tehnoloogiate kohta, lk 8. Vt ka punkt 26 eespool.
[98] Isikuandmete kaitse üldmääruse põhjendus 4. Vt ka artikli 29 töörühma arvamus 3/2012 biomeetriliste tehnoloogiate kohta, lk 8.

ainult siis, kui reisija ilmub lähtelennujaama eelnevalt kindlaksmääratud kontrollpunktidesse, kuid andmete töötlemine toimub keskandmebaasiga ühendatud keskserveris. Selle stsenaariumi puhul on säilitamistähtaeg tavaliselt 48 tundi ja andmed kustutatakse pärast lennuki õhkutõusmist.

Euroopa Andmekaitsenõukogu hinnang

68. Nagu eespool märgitud, kaasneb biomeetriliste andmete töötlemisega suurem oht andmesubjektide õigustele ja vabadustele[99]. Seega võivad mis tahes andmeturbetõrgetel olla andmesubjektidele eriti rasked tagajärjed[100]. Vastutavad töötlejad on kohustatud neid riske tõhusalt maandama. Kuna selle stsenaariumi puhul on kogu arhitektuur täielikult tsentraliseeritud, kaotavad reisijad kontrolli oma andmete üle suuremal määral. Lisaks võib suureneda ka oht, et andmeid töödeldakse muudel eesmärkidel, mis ei ole seotud reisijatevoo kontrollimisega.

69. Pidades silmas turvalisuse põhimõtet ja nõudeid (IKÜM artikli 5 lõike 1 punkt f ja artikkel 32), tuleks arvesse võtta, et isiku- ja biomeetriliste andmete säilitamine kesksetes, kuigi eraldiasuvates andmebaasides võib anda võimaluse ohtlikeks rünneteks ning sellise andmebaasi konfidentsiaalsuse rikkumine võib hiljem kaasa tuua juurdepääsu kogu andmekogumile. Selle tulemusena võib võimalik rikkumine näotuvastusmallide ja nendega seotud isikutuvastusandmetega võimaldada andmesubjekte loata või ebaseaduslikult tuvastada muudes keskkondades. Sõltuvalt biomeetriliseks tuvastamiseks kasutatavatest meetoditest võib see ohustada näotuvastusmallide edasist ohutut kasutamist identifitseerimistunnusena. Sellisel juhul ei saa rikkumise mõju leevendada, erinevalt teist liiki mandaatidest (nt kasutajatunnus, salasõna), mida on võimalik muuta[101].

70. Lisaks muudab vastutava töötleja valduses olevate isiku- ja biomeetriliste andmete suur hulk ja kvaliteet selle ründaja jaoks väga väärtuslikuks sihtmärgiks, millega kaasnevad tõenäolisemad julgeolekuohud. Lisaks võib andmetega seotud rikkumistel olla suurem mõju, sest kui andmeid säilitatakse tsentraliseeritult, võib ründajatel olla lihtsam pääseda ligi paljude reisijate isikuandmetele. Seega võib võimalik rikkumine tuua suure hulga andmesubjektide jaoks kaasa suure raskusastmega ohud, näiteks ulatusliku identiteedivarguse ohu, mida on äärmiselt raske maandada.

71. Seega, pidades silmas kooskõla IKÜM artikli 5 lõike 1 punktiga f ja artikliga 32, ei ole stsenaariumis 3.1[102] kavandatud meetmed tehnoloogia arengut arvesse võttes piisavad, et tagada ohule vastav turvalisuse tase. Selle põhjal ei oleks stsenaariumis 3.1 kirjeldatud töötlemine kooskõlas IKÜM artikli 5 lõike 1 punktiga f ja artikliga 32, kui vastutav töötleja nende meetmetega piirdub.

72. Võttes arvesse IKÜM artikli 5 lõike 1 punktis e sätestatud põhimõtet, on selle stsenaariumi puhul biomeetriliste andmete keskandmebaasis säilitamise aeg tavaliselt 48 tundi. Näib, et selline säilitamise piirang vähendab märkimisväärselt isikuandmetega seotud rikkumistega seotud ohte. Andmete säilitamise aeg ei ole siiski nimetatud arhitektuuri üldise vastavuse seisukohast iseenesest määrav tegur, kuna vastutavad töötlejad võivad selliseid säilitamisperioode muuta. Igal juhul peavad

[99] Vt eespool punkt 26.
[100] Suunised näotuvastuse kohta, Euroopa Nõukogu isiku kaitset isikuandmete automatiseeritud töötlemisel käsitleva konventsiooni konsultatiivkomitee, juuni 2021, lk 22.
[101] Vt ka artikli 29 töörühma arvamus 3/2012 biomeetriliste tehnoloogiate kohta, lk 34.
[102] Nagu on kirjeldatud eespool punktides 64-67.

kavandatud meetmed vastama IKÜM artiklis 25 sätestatud lõimitud andmekaitse ja vaikimisi andmekaitse nõuetele.

73. Erinevalt 1. ja 2. stsenaariumist, kus reisijad autenditakse, toimub stsenaariumi 3.1 puhul reisijate tuvastamine (1:N võrdlus), N on lennujaamas mitme päeva jooksul eeldatav reisijate arv, kes on nõustunud lennujaamas asuvate konkreetsete kontrollpunktide läbimisel sellise töötlemisega. See tähendab reisija kohta keskandmebaasis päringu tegemist ja iga salvestatud biomeetrilise malli töötlemist, et kontrollida, kas see vastab süsteemile teadaolevale isikule. Erinevalt 2. stsenaariumist ei ole stsenaariumi 3.1 puhul võtmed üksnes reisijate käes. Sellest tulenevalt on reisijatel selle stsenaariumi puhul oma biomeetriliste andmete üle oluliselt väiksem kontroll. Seetõttu ei saa selline töötlemine, nagu on kavandatud stsenaariumis 3.1, olla kooskõlas IKÜM artikli 25 kohaste lõimitud andmekaitse ja lõimitud andmekaitse nõuetega.

74. IKÜM artiklit 25 silmas pidades peaksid vastutavad töötlejad kaaluma, mis liiki ja mis kategooriasse kuuluvaid isikuandmeid on vaja töödelda ja missugune peaks olema nende üksikasjalikkuse tase[103]. Kavandamisel tuleks arvesse võtta, et suurel hulgal üksikasjalike isikuandmete kogumisel on võimalikult väheste andmete kogumise, tervikluse, konfidentsiaalsuse ja säilitamise piiramise põhimõtteid raskem järgida, ning võrrelda seda väiksemate ohtudega juhul, kui andmesubjektide kohta kogutakse vähem andmeid ja/või vähem üksikasjalikku teavet. Igal juhul ei tohiks vaikimisi koguda selliseid isikuandmeid, mis ei ole konkreetse töötlemiseesmärgi jaoks vajalikud. Teisisõnu, kui teatavad isikuandmete kategooriad ei ole vajalikud või kui üksikasjalikke andmeid ei ole vaja, sest üldisemad andmed on piisavad, ei tohiks liigseid isikuandmeid koguda. Seega, kui muu töötlemisega saavutataks sama eesmärk ja see on stsenaariumis 3.1 kirjeldatud tingimustel teostatav, ei ole näotuvastustehnoloogia kasutamine vajalik.

75. IKÜM artikli 25 kohaselt on peamine lõimitud andmekaitse ja vaikimisi andmekaitse element andmesubjekti autonoomia. Eelkõige tuleks andmesubjektile anda võimalikult suur autonoomia otsustamisel oma isikuandmete kasutamise üle, samuti sellise kasutamise või töötlemise ulatuse ja tingimuste üle[104]. 1. stsenaariumi puhul oleks andmesubjekt autonoomne ja tal oleks kontroll oma biomeetriliste mallide kasutamise, avalikustamise ja kustutamise üle ning 2. stsenaariumi puhul säilitaks andmesubjekt teatava kontrolli oma biomeetrilise malli avalikustamise üle, kuna krüpteerimisvõti/saladus on tema valduses. Kuid stsenaariumi 3.1 puhul sõltub andmesubjekt oma biomeetriliste andmete töötlemisel täielikult vastutava töötleja valikutest ja seetõttu ei ole tal otsest kontrolli oma biomeetrilise malli kasutamise üle.

76. Pidades silmas kooskõla IKÜM artikliga 25 ja eelkõige nõuet koguda võimalikult väheseid andmeid, ei vasta stsenaariumis 3.1 kavandatud töötlemine vajalikkuse põhimõttele. Andmekaitsenõukogu leiab, et sarnast tulemust reisijatevoo sujuvamaks muutmisel lennujaamades on võimalik saavutada eraelu puutumatusse vähem sekkuval viisil. Näiteks on seda võimalik saavutada ilma biomeetrilisi andmeid kasutamata (kuigi kasutajakogemus oleks sel juhul erinev, sest pardakaardi ja vajaduse korral ametlike isikut tõendavate dokumentide näitamine võib võtta kauem aega). Lisaks võimaldavad muud lahendused, eelkõige need, mille aluseks on biomeetriliste andmete säilitamine isiklikus digitaalses

[103] Euroopa Andmekaitsenõukogu suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse, punkt 49.
[104] Euroopa Andmekaitsenõukogu suunised 4/2019. Lõimitud andmekaitse ja vaikimisi andmekaitse, punkt 70. Isikuandmete kaitse üldmääruse põhjenduses 7 on täiendavalt selgitatud, et „[f]üüsilistel isikutel peaks olema kontroll oma isikuandmete üle“.

rahakotis üksikisiku seadmes, või mis nõuavad andmete krüpteerimist konkreetse võtmega, mis on salvestatud üksikisiku seadmesse, saavutada eesmärgid eraelu puutumatusse vähem sekkuval viisil.

77. Proportsionaalsuse põhimõtet silmas pidades ohustaks stsenaariumis 3.1 kavandatud töötlemine andmesubjektide õigusi ja seda ei saaks tehnoloogia arengut arvestades leevendada. Oht, et suure hulga üksikisikute biomeetriliste andmete keskandmebaasis säilitatavate andmetega seotud rikkumine võib avaldada andmesubjektide põhiõigustele ja -vabadustele negatiivset mõju, näib kaaluvat üles töötlemisest tuleneva eeldatava kasu, kuna selline kasu on suhteliselt väike, st kontrollide mugavus ja kiirus suureneb mõnevõrra . Seega ei saa see õigustada nende meetmete suurt sekkuvust üksikisikute põhiõiguste ja -vabaduste seisukohast ning stsenaariumis 3.1 ette nähtud töötlemine ei vasta proportsionaalsuse põhimõttele.

78. Neid kaalutlusi arvesse võttes järeldab andmekaitsenõukogu vastuses küsimusele 2.2.1, et kui töötlemine toimub konkreetselt selleks, et reisijatevoogu lennujaamades sujuvamaks muuta, siis stsenaariumis 3.1 kavandatud töötlemine:

- **ei ole kooskõlas IKÜM artikliga 25;**
- **ei oleks kooskõlas IKÜM artikli 5 lõike 1 punktiga f ja artikliga 32** ka juhul, kui vastutav töötleja piirduks stsenaariumis 3.1 kirjeldatud meetmetega.

3.2.3.2 Stsenaarium 3.2: tsentraliseeritud säilitamine pilves, lennufirma kontrolli all

Stsenaariumi kirjeldus

79. Stsenaariumi 3.2 puhul säilitatakse reisijate registreeritud biomeetrilist malli pilves lennufirma või tema pilveteenuse osutaja (volitatud töötleja) kontrolli all. Taotluses on täpsustatud, et pilveteenuse osutaja asub EMPs[105]. Sellisel juhul on reisijate andmed krüpteeritud ja dekrüpteeritakse kasutamise ajaks (näiteks võrdlustoimingu tegemisel), ning võtmeid kontrollib lennufirma või tema pilveteenust osutav volitatud töötleja. Reisijate biomeetrilisi andmeid kasutatakse reisijate tuvastamiseks (1:N võrdlus), kus N võib ulatuda lennufirma klientide koguarvuni[106].

80. Sarnaselt stsenaariumidega 1, 2 ja 3.1 peavad ka reisijad kõigepealt registreeruma. Stsenaariumi 3.2 puhul toimub reisijate registreerimine siiski ühekordselt ja kehtib seni, kuni kliendil on lennufirma juures konto. Registreerimine toimub kas kaugühenduse kaudu asjakohasel isikusamasuse usaldusväärsuse tagamise tasemel (nt eIDASe asjakohane usaldusväärsuse tase) või lennujaamaterminalides. Biomeetriline võrdlemine toimub ainult siis, kui reisija ilmub lennujaama eelnevalt kindlaksmääratud kontrollpunktidesse, kuid andmete töötlemine toimub pilves.

81. Lennujaamas läbivad reisijad spetsiaalsed kontrollseadmed, mis on varustatud kaameraga. Reisijate biomeetrilised andmed saadetakse päringu kaudu lennufirma pilveserverisse, kus neid võrreldakse keskandmebaasis olevatega. Seega on võimalik reisija tuvastada ja kontrollida, kas ta on tõepoolest väljuvale lennule (või pardalemineku kontrolli korral lennule, mille pardale minek parajasti toimub) registreeritud.

82. Kui lennufirmal on spetsiaalne terminal või juurdepääs lennujaama ühisele infosüsteemi taristule, võib võrdluse tulemused teha kättesaadavaks mitmele lennujaama käitajale. Sõltuvalt kontrollpunktist võib päringu esitanud kontrollpunkti vastutavale töötlejale tagasi saadetud andmeid minimeerida, piirdudes näiteks „jah/ei“ vastuse või vajaduse korral võrdlustulemusega. Sellisel juhul näeb kontrollpunkti vastutav töötleja ainult päringu tulemust ja ainult seda ta kasutabki.

83. Malli säilitamistähtaja määrab kindlaks lennufirma ja see võib kesta seni, kuni kliendil on lennufirma juures konto.

Euroopa Andmekaitsenõukogu hinnang

84. Andmekaitsenõukogu poolt seoses stsenaariumiga 3.1 juba väljendatud kaalutlused[107] kehtivad ka selle stsenaariumi kohta.

85. Mis puudutab turvalisuse põhimõtet ja nõudeid (IKÜM artikli 5 lõike 1 punkt f ja artikkel 32), siis toimub stsenaariumi 3.2 puhul töötlemine pilves ja sellistele andmetele võib olla juurdepääs paljudel üksustel, sealhulgas EMP-välistel teenuseosutajatel, isegi kui andmeid hoitakse EMPs[108]. Sellise

[105] Prantsusmaa järelevalveasutus selgitas, et see on näitlik ja et kaaluda võiks ka pilveteenuse osutajaid, kelle asukoht ei ole EMPs. Lisaks võiks kavandada ka muid säilituslahendusi (nt pilvandmetöötluseta).
[106] Prantsusmaa järelevalveasutus selgitas, et see on näitlik ja on olemas lahendus, kus biomeetrilisi andmeid edastatakse iga kord enne lendu.
[107] Punktid 68–77 eespool.
[108] Euroopa Andmekaitsenõukogu 2022. aasta koordineeritud jõustamismeede pilvteenuste kasutamiseks avalikus sektoris, 17. jaanuar 2023, lk 19.

arhitektuuriga kaasnevad võimalikud ohud seoses isikuandmete edastamisega kolmandatesse riikidesse. Kuigi sellisel juhul on reisijate andmed krüpteeritud, dekrüpteeritakse need kasutamise ajaks (st võrdlustoimingu tegemisel), ning võtmeid kontrollib lennufirma või talle pilveteenust osutav volitatud töötleja. Selline säilitamine võib kaasa tuua suuremad turvaprobleemid tulevikus.

86. Seega, pidades silmas kooskõla IKÜM artikli 5 lõike 1 punktiga f ja artikliga 32, ei ole stsenaariumis 3.2[109] kavandatud meetmed tehnika arengut arvesse võttes piisavad, et tagada ohule vastav turvalisuse tase. Selle põhjal ei oleks stsenaariumi 3.2 kohane töötlemine kooskõlas IKÜM artikli 5 lõike 1 punktiga f ja artikliga 32, kui vastutav töötleja nende meetmetega piirdub.

87. Lisaks võib stsenaariumi 3.2[110] kohaselt andmeid säilitada märkimisväärse aja jooksul (st põhimõtteliselt nii kaua, kuni andmesubjektil on lennufirma juures konto). Sellise säilitamistähtaja tõttu on andmete konfidentsiaalsuse ja tervikluse rikkumise oht suurem ning tundub, et see läheb kaugemale sellest, mis on töötlemise eesmärgil rangelt vajalik ja proportsionaalne. Andmekaitsenõukogu märgib, et andmete säilitamistähtaeg ei ole siiski määrav tegur, kas nimetatud arhitektuur on vastavuses IKÜMiga , kuna vastutavad andmetöötlejad võivad selliseid säilitusperioode muuta. Andmekaitsenõukogu käsutuses oleva ja stsenaariumi 3.2 kirjelduses sisalduva teabe põhjal ei ole see pikk säilitamistähtaeg siiski piisavalt põhjendatud ja puuduvad nähtavad meetmed üksikisikutele avalduvate riskide maandamiseks. Sellest tulenevalt ei piirduks kavandatav säilitamistähtaeg IKÜM artikli 5 lõike 1 punktis e sätestatud säilitamise piiramise põhimõtte kohaselt vajalikuga.

88. Igal juhul ei vasta stsenaariumi 3.2 puhul kavandatud meetmed IKÜM artiklis 25 sätestatud lõimitud ja vaikimisi andmekaitse nõuetele. Stsenaariumi 3.2 puhul säilitatakse reisijate registreeritud biomeetrilisi malle pilves lennufirma või tema pilveteenuse osutaja (volitatud töötleja) kontrolli all. Nagu eespool kirjeldatud, võivad nendele andmetele juurde pääseda mitmed üksused. Lisaks kasutatakse reisijate biomeetrilisi andmeid reisijate tuvastamiseks (1:N võrdlus), kus N võib ulatuda lennufirma kasutajate/klientide koguarvuni. Selline meetod tähendab isiku leidmist keskandmebaasis oleva isikute rühma hulgast, töödeldes iga salvestatud näopilti, et kontrollida, kas see langeb kokku süsteemile teadaoleva isikuga. Erinevalt stsenaariumist 3.1 oleks stsenaariumi 3.2 puhul võimalik võrrelda palju suuremas ulatuses, kuna siin on kriteeriumiks lennufirma klientide koguarv, samas kui stsenaarium 3.1 hõlmas ainult mõne päeva jooksul eeldatavat reisijate arvu.

89. Pidades silmas kooskõla IKÜM artikliga 25 ja eelkõige nõuet koguda võimalikult väheseid andmeid, ei vasta stsenaariumis 3.2 kavandatud töötlemine ka vajalikkuse põhimõttele. Andmekaitsenõukogu leiab, et sarnast tulemust lennujaamade reisijatevoo sujuvamaks muutmisel oleks võimalik saavutada muude vähem sekkuvate meetmetega, näiteks biomeetrilisi andmeid kasutamata, kuigi kasutajakogemus oleks sel juhul teistsugune, sest isikut tõendava dokumendi ja pardakaardi näitamine võib võtta kauem aega. Lisaks võimaldavad muud lahendused, eelkõige need, mille aluseks on biomeetriliste andmete säilitamine isiklikus digitaalses rahakotis üksikisiku seadmes, või mis nõuavad andmete krüpteerimist konkreetse võtmega, mis on salvestatud üksikisiku seadmesse, saavutada vastutaval töötlejal oma eesmärgid viisil, mis sekkub vähem eraelu puutumatusse.

[109] Vt eespool punktid 79–83.
[110] Vt punkt 83 eespool.

90. Proportsionaalsuse põhimõtet silmas pidades ohustaks stsenaariumis 3.2 kavandatud töötlemine andmesubjektide õigusi ja seda ei saaks kavandatud kaitsemeetmetega leevendada. Rikkumine, mis võib tekkida pilves asuvas keskandmebaasis, mis sisaldab suurt hulka üksikisikute biomeetrilisi andmeid avaldaks andmesubjektide põhiõigustele ja -vabadustele negatiivset mõju, mis näib kaaluvat üles töötlemisest tuleneva eeldatava kasu, kuna selline kasu on suhteliselt väike, st mõnevõrra suureneb kontrollide mugavus ja kiirus. Seega ei saa see õigustada nende meetmete suurt sekkuvust üksikisikute põhiõiguste ja -vabaduste vaatest ning stsenaariumis 3.2 ette nähtud töötlemist ei saa pidada proportsionaalseks.

91. Neid kaalutlusi arvesse võttes järeldab andmekaitsenõukogu vastuses küsimusele 2.3.1, et kui töötlemine toimub konkreetselt selleks, et reisijatevoogu lennujaamades sujuvamaks muuta, siis stsenaariumis 3.2 kavandatud töötlemine:

- **ei ole kooskõlas IKÜM artikliga 25;**
- **ei oleks kooskõlas IKÜM artikli 5 lõike 1 punktiga f ja artikliga 32** ka juhul, kui vastutav töötleja piirduks stsenaariumis 3.2 kirjeldatud meetmetega;
- **ei oleks kooskõlas IKÜM artikli 5 lõike 1 punktiga e**, kuna stsenaariumis 3.2 ette nähtud säilitamistähtaeg ei ole andmekaitsenõukogu käsutuses oleva teabe põhjal piisavalt põhjendatud. IKÜM artikli 5 lõike 1 punktis e sätestatud säilitamise piiramise põhimõtte järgimiseks peaks vastutav töötleja tõendama, et isikuandmeid ei säilitata kauem, kui on vajalik nende töötlemise eesmärgi saavutamiseks.

4 JÄRELDUSED

92. Prantsusmaa JVA arvamustaotluse põhjal seoses küsimusega 1.1 IKÜM artikli 5 lõike 1 punktis f ning artiklites 25 ja 32 sätestatud nõuete kohta ning eespool esitatud analüüsi alusel järeldab andmekaitsenõukogu, et:

93. näotuvastustehnoloogia kasutamist biomeetriliseks autentimiseks lennujaamades reisijatevoo sujuvamaks muutmise eesmärgil (julgestuskontroll, pagasi äraandmine, pardaleminek ja juurdepääs reisijate *lounge*'ile) võiks pidada IKÜM artikli 5 lõike 1 punktiga f, artiklitega 25 ja 32 põhimõtteliselt kooskõlas olevaks, kui kasutatakse säilitusarhitektuuri, mille puhul iga reisija registreeritud biomeetrilist malli säilitatakse üksnes üksikisiku valduses olevas isiklikus seadmes, mis on tema ainukontrolli all, kui rakendatakse asjakohaseid kaitsemeetmeid, mida on kirjeldatud eespool punktis 46.

94. Prantsusmaa JVA arvamustaotluse põhjal seoses küsimusega 2.1.1 IKÜM artikli 5 lõike 1 punktides e ja f ning artiklites 25 ja 32 sätestatud nõuete kohta ning eespool esitatud analüüsi põhjal järeldab andmekaitsenõukogu, et:

95. näotuvastustehnoloogia kasutamist biomeetrilise autentimise eesmärgil reisijatevoo ühtlustamiseks lennujaamades (julgestuskontrollipunktid, pagasi äraandmine, pardaleminek ja juurdepääs reisijate *lounge*'ile) võib põhimõtteliselt pidada IKÜM artikli 5 lõike 1 punktis e sätestatud säilitamise piirangu põhimõttega ning artikli 5 lõike 1 punkti f kohaste usaldusväärsuse ja konfidentsiaalsuse põhimõtetega ning IKÜM artiklitega 25 ja 32 kooskõlas olevaks, kui kasutatakse tsentraliseeritud säilitusarhitektuuri, mille puhul iga reisija registreeritud biomeetrilist malli säilitatakse lennujaama keskses andmebaasis, lennujaama käitaja kontrolli all, krüpteeritud kujul, ning võti/saladus on üksnes üksikisiku käes, kui kohaldatakse eespool punktis 60 kirjeldatud asjakohaseid kaitsemeetmeid.

96. Prantsusmaa JVA arvamustaotluse põhjal seoses küsimusega 2.2.1 IKÜM artikli 5 lõike 1 punktides e ja f ning artiklites 25 ja 32 sätestatud nõuete kohta ning eespool esitatud analüüsi põhjal järeldab andmekaitsenõukogu, et:

97. IKÜM artikliga 25 ei ole kooskõlas näotuvastustehnoloogia kasutamine biomeetriliseks tuvastamiseks, mida kasutatakse lennujaamades reisijatevoo sujuvamaks muutmise eesmärgil (julgestuskontrollpunktid, pagasi äraandmine, pardaleminek ja juurdepääs reisijate *lounge*'ile), kui kasutatakse tsentraliseeritud säilitusarhitektuuri, mille puhul reisijate registreeritud biomeetrilised mallid ei ole krüpteeritud võtmega/saladusega, mis on üksnes iga reisija valduses, kui selliseid malle säilitatakse lennujaamas asuvas andmebaasis (lennujaama käitaja kontrolli all). Selline töötlemine ei oleks kooskõlas IKÜM artikli 5 lõike 1 punktis f sätestatud usaldusväärsuse ja konfidentsiaalsuse põhimõttega ja artikliga 32 ka juhul, kui vastutav töötleja piirduks stsenaariumis 3.1 kirjeldatud meetmetega.

98. Seoses küsimusega 2.3.1 järeldab andmekaitsenõukogu Prantsusmaa JVA arvamustaotluse põhjal seoses IKÜM artikli 5 lõike 1 punktides e ja f ning artiklites 25 ja 32 sätestatud nõuetega ning eespool esitatud analüüsi alusel, et:

99. IKÜM artikliga 25 ei ole kooskõlas näotuvastustehnoloogia kasutamine biomeetriliseks tuvastamiseks, mida kasutatakse lennujaamades reisijatevoo sujuvamaks muutmise eesmärgil (julgestuskontrollpunktid, pagasi äraandmine, pardaleminek ja juurdepääs reisijate *lounge*'ile), kui kasutatakse tsentraliseeritud säilitusarhitektuuri, mille puhul reisijate registreeritud biomeetrilised mallid ei ole krüpteeritud üksnes iga reisija valduses oleva võtmega/saladusega ja neid malle säilitatakse pilves (lennufirma kontrolli all). Selline töötlemine ei oleks kooskõlas IKÜM artikli 5 lõike 1 punktis f sätestatud usaldusväärsuse ja konfidentsiaalsuse põhimõtetega ja artikliga 32 ka juhul, kui vastutav töötleja piirduks stsenaariumis 3.2 kirjeldatud meetmetega. Samuti ei oleks stsenaariumi 3.2 kirjelduse ja andmekaitsenõukogule kättesaadava teabe põhjal töötlemine kooskõlas IKÜM artikli 5 lõike 1 punktis e sätestatud säilitamise piirangu põhimõttega.

Euroopa Andmekaitsenõukogu nimel

eesistuja

(Anu Talus)