Tietosuojaneuvoston lausunto (64 artikla)

Lausunto 11/2024 kasvojentunnistuksen käytöstä lentoasemien matkustajavirtojen sujuvoittamiseksi (yhteensopivuus yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa)

Versio 1.1

Annettu 23. toukokuuta 2024

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

Hyväksytty

Versio 1.1	28.5.2024	Kieliopillinen oikaisu tiivistelmään (sivut 3 ja 4) ja lausunnon 77 ja 90 kohtaan
Versio 1.0	23.5.2024	Lausunnon hyväksyminen

Tiivistelmä

Ranskan valvontaviranomainen pyysi Euroopan tietosuojaneuvostoa antamaan lausunnon siitä, miten lentoasemien pitäjät ja lentoyhtiöt käyttävät kasvojentunnistusteknologiaa matkustajien henkilöllisyyden biometriseen todentamiseen tai matkustajien tunnistamiseen lentoasemien matkustajavirtojen sujuvoittamiseksi.

Tietosuojaneuvosto muistuttaa alustavana huomautuksena, että biometristen tietojen ja erityisesti kasvojentunnistusteknologian käyttö lisää rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä. Se liittyy biometristen tietojen käsittelyyn, joille on myönnetty erityinen suoja yleisen tietosuoja-asetuksen 9 artiklan nojalla. Vaikka tällaisten teknologioiden käyttöä pidettäisiin erityisen tehokkaana, rekisterinpitäjien olisi ennen niiden käyttämistä arvioitava rekisteröityjen perusoikeuksiin ja -vapauksiin kohdistuvia vaikutuksia ja pohdittava, voitaisiinko käsittelyn laillinen tarkoitus saavuttaa yksityisyyteen vähemmän puuttuvilla keinoilla.

Tämän lausunnon soveltamisala rajoittuu pyynnön mukaisesti käsittelyn yhteensopivuuteen **yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa**, kun käsittelyn **nimenomaisena tarkoituksena on sujuvoittaa matkustajavirtoja lentoasemilla** neljässä tarkastuspisteessä eli turvatarkastuspisteissä, matkatavaroiden jättöpisteissä, koneeseen siirryttäessä ja matkustajien lounge-tilojen sisäänkäynnissä. Tässä lausunnossa ei tehdä kattavaa analyysiä siitä, noudattavatko asianomaiset rekisterinpitäjät ja soveltuvin osin niiden henkilötietojen käsittelijät yleistä tietosuoja-asetusta kussakin tapauksessa. Näin ollen tämä lausunto ei vaikuta tapauskohtaiseen oikeudelliseen ja tekniseen analyysiin, joka perustuu rekisterinpitäjän kussakin tapauksessa suunnittelemaan käsittelyyn ja olosuhteisiin. Sovellettavan oikeusperusteen analysointi ei myöskään kuulu pyynnössä tietosuojaneuvostolle esitettyjen kysymysten piiriin, ja tästä syystä tässä lausunnossa ei tarkastella yleisen tietosuoja-asetuksen 6, 7 ja 9 artiklan mukaisen käsittelylle annetun suostumuksen pätevyyttä. Tämä lausunto ei myöskään vaikuta jäsenvaltioiden lainsäädännössä säädettyihin biometristen tietojen käyttöä koskeviin rajoituksiin.

Tietosuojaneuvosto arvioi tässä lausunnossa, onko käsittely edellä mainittujen yleisen tietosuoja-asetuksen säännösten mukaista **neljässä erityisessä skenaariossa**.

Ensimmäisessä skenaariossa rekisteröity biometrinen malli säilytetään henkilön hallussa, esimerkiksi hänen henkilökohtaisella laitteellaan, ja hänen yksinomaisessa valvonnassaan matkustajan henkilöllisyyden todentamista varten (yksi yhteen -vertailu) hänen kulkiessaan edellä mainittujen lentoaseman tarkastuspisteiden läpi.

Tietosuojaneuvosto päättelee, että valittujen toimenpiteiden voitaisiin katsoa olevan tarpeellisuuden periaatteen mukaisia, jos rekisterinpitäjä voi osoittaa, ettei ole olemassa yksityisyyteen vähemmän puuttuvia vaihtoehtoisia ratkaisuja, joilla sama tavoite voitaisiin saavuttaa yhtä tehokkaasti. Lisäksi käsittelyn yksityisyyteen puuttumisen astetta voidaan tasapainottaa matkustajien aktiivisella osallistumisella, koska heidän biometrinen mallinsa tallennetaan vain heidän haltuunsa, esimerkiksi heidän henkilökohtaiselle laitteelleen, se on vain heidän valvonnassaan ja heidän tietonsa poistetaan pian sen jälkeen, kun mallin vertailu on saatu päätökseen. Tämän perusteella tietosuojaneuvosto päättelee, että ensimmäisessä skenaariossa suunniteltua käsittelyä **voitaisiin periaatteessa pitää yhteensopivana yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan, 25 artiklan ja 32 artiklan kanssa**, mikäli toteutetaan asianmukaiset suojatoimet.

Tietosuojaneuvosto on yksilöinyt suojatoimia, jotka vähintään olisi toteutettava ensimmäisen skenaarion kaltaisessa ratkaisussa.

Toisessa skenaariossa rekisteröity biometrinen malli säilytetään lentoasemalla keskitetysti salatussa muodossa, jonka avain/salasana on vain matkustajan hallussa. Tämä mahdollistaa matkustajan henkilöllisyyden todentamisen (yksi yhteen -vertailu) hänen kulkiessaan edellä mainittujen lentoaseman tarkastuspisteiden läpi. Rekisteröinti on voimassa tietyn ajan, esimerkiksi enintään yhden vuoden viimeisen lennon jälkeen passin voimassaolon päättymispäivään asti.

Tietosuojaneuvosto päättelee, että käsittelyn voitaisiin katsoa olevan tarpeellisuuden periaatteen mukaista, jos rekisterinpitäjä voi osoittaa, ettei ole olemassa yksityisyyteen vähemmän puuttuvia vaihtoehtoisia ratkaisuja, joilla sama tavoite voitaisiin saavuttaa yhtä tehokkaasti. Lisäksi käsittelyn yksityisyyteen puuttumisen astetta voidaan tasapainottaa matkustajien aktiivisella osallistumisella, koska salattujen biometristen tietojen avain/salasana on vain heidän valvonnassaan. Mikäli rekisterinpitäjä toteuttaa asianmukaiset suojatoimet, keskitetyn tietokannan käytöstä tässä skenaariossa aiheutuvia turvallisuusriskejä voitaisiin lieventää ja rekisteröityjen perusoikeuksiin ja -vapauksiin kohdistuvaa kielteistä vaikutusta voitaisiin pitää oikeasuhteisena ennakoituun hyötyyn nähden. Säilytyksen rajoittamista koskevan periaatteen osalta tietosuojaneuvostolle ei ole toimitettu tietoja, joilla voitaisiin perustella pitkä säilytysaika. Jotta tämä skenaario olisi yhteensopiva yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan kanssa, rekisterinpitäjien olisi pystyttävä perustelemaan, miksi suunniteltu säilytysaika on tarpeen kussakin tapauksessa kyseessä olevaa tarkoitusta varten. Tietosuojaneuvosto suosittelee, että rekisterinpitäjät suunnittelevat mahdollisimman lyhyitä säilytysaikoja ja tarjoavat matkustajille mahdollisuuden valita haluamansa säilytysajan. Tämän perusteella tietosuojaneuvosto päättelee, että toisessa skenaariossa suunniteltua käsittelyä **voitaisiin periaatteessa pitää yhteensopivana yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan, 25 artiklan ja 32 artiklan kanssa**, mikäli toteutetaan asianmukaiset suojatoimet.

Tietosuojaneuvosto on yksilöinyt suojatoimia, jotka vähintään olisi toteutettava toisen skenaarion kaltaisessa ratkaisussa.

Kolmannessa skenaariossa rekisteröity biometrinen malli säilytetään keskitetysti salatussa muodossa lentoasemalla lentoaseman pitäjän valvonnassa. Tämä mahdollistaa matkustajan tunnistamisen (1:N-eli yksi moneen -vertailu) hänen kulkiessaan edellä mainittujen lentoaseman tarkastuspisteiden läpi. Tässä skenaariossa säilytysaika on tavallisesti 48 tuntia, ja tiedot poistetaan lentokoneen lähdettyä.

Koska tunnistetiedot ja biometriset tiedot tallennetaan keskustietokantaan, tietokannan luottamuksellisuuden vaarantuminen saattaa johtaa siihen, että kaikki tiedot ovat saatavilla, ja mahdollistaa matkustajien luvattoman tai laittoman tunnistamisen muissa ympäristöissä. Lentoaseman pitäjän valvonnassa oleva keskitetty tallennusrakenne johtaa myös siihen, että matkustajat menettävät suuremmassa määrin mahdollisuuden valvoa tietojaan. Tietosuojaneuvosto katsoo, että samankaltainen tulos lentoasemien matkustajavirtojen sujuvoittamiseksi voidaan saavuttaa yksityisyyteen vähemmän puuttuvalla tavalla ja että keskitettyyn biometrisiä tietoja sisältävään tietokantaan kohdistuvasta tietoturvaloukkauksesta aiheutuva kielteinen vaikutus rekisteröityjen perusoikeuksiin ja -vapauksiin näyttäisi olevan suurempi kuin käsittelystä odotettavissa oleva hyöty. Sen vuoksi käsittely ei voi olla tarpeellisuuden ja oikeasuhteisuuden periaatteiden mukaista. Tämän perusteella tietosuojaneuvosto päättelee, että kolmannessa skenaariossa hahmoteltu käsittely **ei voi olla yhteensopivaa yleisen tietosuoja-asetuksen 25 artiklan kanssa**. Se **ei olisi myöskään yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan kanssa**, jos rekisterinpitäjä toteuttaisi vain tässä skenaariossa kuvatut toimenpiteet.

<u>Neljännessä skenaariossa</u> rekisteröity biometrinen malli tallennetaan keskitetysti salatussa muodossa pilvipalveluun, joka on lentoyhtiön tai sen pilvipalveluntarjoajan valvonnassa. Tämä mahdollistaa matkustajan tunnistamisen (1:N- eli yksi moneen -vertailu) hänen kulkiessaan edellä mainittujen lentoaseman tarkastuspisteiden läpi. Tässä skenaariossa tietoja on mahdollista säilyttää niin kauan kuin asiakkaalla on tili lentoyhtiössä.

Koska tunnistetiedot ja biometriset tiedot tallennetaan pilvipalvelun keskustietokantaan, useilla toimijoilla, mahdollisesti myös ETA:n ulkopuolisilla palveluntarjoajilla, saattaisi olla pääsy tällaisiin tietoihin. Matkustajan tietojen salaus puretaan, kun niitä käytetään, ja avaimet ovat lentoyhtiön tai sen tietojenkäsittelijöiden valvonnassa, mikä voi lisätä turvallisuusuhkien mahdollisuutta. Tällainen keskitetty tallennusrakenne johtaa myös siihen, että matkustajat menettävät suuremmassa määrin mahdollisuuden valvoa tietojaan. Tietoja voidaan myös säilyttää huomattavan kauan, minkä vuoksi niihin kohdistuva tietoturvaloukkausten riski on suurempi, ja säilytysaika näyttäisi olevan pidempi kuin käsittelyn kannalta on ehdottoman välttämätöntä ja oikeasuhteista, ellei henkilöihin kohdistuvien riskien vähentämiseksi toteuteta ilmeisiä lisätoimenpiteitä.

Tietosuojaneuvosto katsoo, että samankaltainen tulos lentoasemien matkustajavirtojen sujuvoittamiseksi voidaan saavuttaa yksityisyyteen vähemmän puuttuvalla tavalla ja että keskitettyyn biometrisiä tietoja sisältävään tietokantaan kohdistuvasta tietoturvaloukkauksesta aiheutuva kielteinen vaikutus rekisteröityjen perusoikeuksiin ja -vapauksiin näyttäisi olevan suurempi kuin käsittelystä odotettavissa oleva hyöty. Sen vuoksi käsittely ei voi olla tarpeellisuuden ja oikeasuhteisuuden periaatteiden mukaista. Tämän perusteella tietosuojaneuvosto päättelee, että neljännessä skenaariossa hahmoteltu käsittely **ei voi olla yhteensopivaa yleisen tietosuoja-asetuksen 25 artiklan kanssa**. Tietosuojaneuvoston käytettävissä olevien tietojen perusteella **se ei myöskään olisi yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan eikä 32 artiklan kanssa**, jos rekisterinpitäjä toteuttaisi vain tässä skenaariossa kuvatut toimenpiteet.

Sisällysluettelo

Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27. huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, jäljempänä ’**yleinen tietosuoja-asetus**’, 63 artiklan sekä 64 artiklan 2 kohdan,

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018[1],

ottaa huomioon Euroopan tietosuojaneuvoston, jäljempänä ’**tietosuojaneuvosto**’ työjärjestyksen 10 artiklan ja 22 artiklan,

sekä katsoo seuraavaa:

1) Euroopan tietosuojaneuvoston päätehtävänä on varmistaa, että yleistä tietosuoja-asetusta sovelletaan yhdenmukaisesti Euroopan talousalueella, jäljempänä ’**ETA**’. Yleisen tietosuoja-asetuksen 64 artiklan 2 kohdassa säädetään, että jokainen valvontaviranomainen, tietosuojaneuvoston puheenjohtaja tai Euroopan komissio voi pyytää minkä tahansa yleisluonteisen tai useammassa kuin yhdessä jäsenvaltiossa vaikutuksia tuottavan asian käsittelyä tietosuojaneuvostossa lausunnon saamiseksi.

2) Yleisen tietosuoja-asetuksen 64 artiklan 3 kohdan ja tietosuojaneuvoston työjärjestyksen 10 artiklan 2 kohdan mukaan tietosuojaneuvoston on hyväksyttävä lausuntonsa kahdeksan viikon kuluessa siitä päivästä, jona tietosuojaneuvoston puheenjohtaja ja toimivaltaiset valvontaviranomaiset ovat päättäneet, että asiakirja-aineisto täyttää kaikki sille asetetut vaatimukset. Määräaikaa voidaan jatkaa puheenjohtajan päätöksellä kuudella viikolla ottaen huomioon asian monimutkaisuus,

on hyväksynyt seuraavan lausunnon:

1 JOHDANTO

1.1 Yhteenveto tosiseikoista

1. Ranskan valvontaviranomainen pyysi 16. helmikuuta 2024 tietosuojaneuvostoa antamaan lausunnon siitä, onko lentoasemien pitäjien ja lentoyhtiöiden harjoittama kasvojentunnistusteknologian käyttö biometriikkaan perustuvaan matkustajien henkilöllisyyden todentamiseen tai matkustajien[2] tunnistamiseen matkustajavirtojen sujuvoittamiseksi lentoasemien turvatarkastuspisteissä[3], matkatavaroiden jättöpisteissä, koneeseen siirryttäessä ja matkustajien lounge-tilojen

[1] Viittauksilla ”**jäsenvaltioihin**” tarkoitetaan tässä lausunnossa ETA:n jäsenvaltioita. Tässä lausunnossa olevia viittauksia unioniin tai EU:hun pidetään viittauksina ETA:an.

[2] Tässä lausunnossa ”**matkustajalla**” tarkoitetaan rekisteröityä, jonka henkilötietoja käsitellään tässä lausunnossa kuvattua erityistarkoitusta varten. Jäljempänä tässä lausunnossa ilmauksia ”matkustaja” ja ”henkilö” käytetään samassa merkityksessä.

[3] Tässä lausunnossa ”**lentoasemien turvatarkastuspisteillä**” tarkoitetaan lentoaseman pitäjän vastuulla suoritettavia turvatarkastuksia, jotka matkustajien on läpäistävä päästäkseen lähtöhallista lähtöporttialueelle tai lähtöportille.

sisäänkäynnissä (lukuun ottamatta rajavalvontaa ja verovapaiden myymälöiden suorittamia tarkastuksia) yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa, jäljempänä '**pyyntö**'. Ranskan valvontaviranomainen liitti pyyntöönsä kuvauksen tyypillisistä käyttötapauksista (liite I).

2. Ranskan valvontaviranomainen huomauttaa pyynnössään, että useilla EU:n lentoasemilla parhaillaan testattavat mallit vaihtelevat jäsenvaltiosta toiseen, mikä voi aiheuttaa riskin siitä, että valvontaviranomaisten tulkinnat eroavat toisistaan, sekä siitä, että rekisteröityjen perusoikeuksiin ja vapauksiin kohdistuvat vaikutukset ovat eri puolilla EU:ta erilaisia.[4]

3. Tietosuojaneuvosto katsoo, että pyyntöön vastaaminen edellyttää seuraavien kysymysten ratkaisemista:

4. **Kysymys 1**:

1.1. Voiko kasvojentunnistusteknologian käyttö biometriikkaan perustuvaan todentamiseen **nimenomaisesti matkustajavirtojen sujuvoittamiseksi lentoasemilla** (turvatarkastuspisteet, matkatavaroiden jättöpisteet, koneeseen siirtyminen ja matkustajien lounge-tilojen sisäänkäynnit) olla yhteensopivaa **yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan, 25 artiklan ja 32 artiklan** kanssa, kun käytetään tallennusrakennetta, jossa kunkin matkustajan biometrinen malli säilytetään **vain kyseisen henkilön hallussa**, esimerkiksi paikallisesti hänen henkilökohtaisella laitteellaan, ja yksinomaan hänen valvonnassaan?

1.2. Jos tällainen käsittely katsottaisiin edellä mainittujen säännösten mukaiseksi, mitä asianmukaisia vähimmäissuojatoimia yleisen tietosuoja-asetuksen 25 ja 32 artiklan perusteella tarvittaisiin?

Kysymys 2:

2.1. Voiko kasvojentunnistusteknologian käyttö biometriikkaan perustuvaan todentamiseen tai tunnistamiseen **nimenomaisesti matkustajavirtojen sujuvoittamiseksi lentoasemilla** (turvatarkastuspisteet, matkatavaroiden jättöpisteet, koneeseen siirtyminen ja matkustajien lounge-tilojen sisäänkäynnit) olla yhteensopivaa **yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan, 25 artiklan ja 32 artiklan** kanssa, kun käytetään keskitettyä tallennusrakennetta, jossa kunkin matkustajan biometrinen malli säilytetään keskitetyssä tietokannassa

2.1.1. lentoaseman pitäjän valvonnassa olevassa ja lentoasemalla sijaitsevassa keskustietokannassa salatussa muodossa, jonka avain/salasana on yksinomaan henkilön hallussa (esimerkiksi matkapuhelimessa) todentamista varten?

2.1.2 Jos tällainen käsittely katsottaisiin säännösten mukaiseksi, mitä asianmukaisia vähimmäissuojatoimia yleisen tietosuoja-asetuksen 25 ja 32 artiklan perusteella tarvittaisiin?

[4] Pyyntö, s. 1.

2.2.1. lentoaseman pitäjän valvonnassa olevassa ja lentoasemalla sijaitsevassa keskustietokannassa salatussa muodossa, jonka avaimet ovat lentoaseman pitäjän hallussa, tunnistamista varten?

2.2.2. Jos tällainen käsittely katsottaisiin säännösten mukaiseksi, mitä asianmukaisia vähimmäissuojatoimia yleisen tietosuoja-asetuksen 25 ja 32 artiklan perusteella tarvittaisiin?

2.3.1. lentoyhtiön tai sen palveluntarjoajan (henkilötietojen käsittelijän) valvonnassa olevassa pilvipalvelussa salatussa muodossa, jonka avaimet ovat lentoyhtiön tai sen palveluntarjoajan hallussa, tunnistamista varten?

2.3.2. Jos tällainen käsittely katsottaisiin säännösten mukaiseksi, mitä asianmukaisia vähimmäissuojatoimia yleisen tietosuoja-asetuksen 25 ja 32 artiklan perusteella tarvittaisiin?

5. Sen jälkeen, kun Ranskan valvontaviranomainen oli 16. helmikuuta 2024 katsonut, että asiakirja-aineisto oli täydellinen ja tietosuojaneuvoston puheenjohtaja oli 23. helmikuuta 2024 katsonut, että asiakirja-aineisto täytti kaikki sille asetetut vaatimukset, sihteeristö jakoi aineiston 23. helmikuuta 2024. Tietosuojaneuvoston puheenjohtaja päätti yleisen tietosuoja-asetuksen 64 artiklan 3 kohdan sekä tietosuojaneuvoston työjärjestyksen 10 artiklan 2 kohdan mukaisesti jatkaa oletusarvoista kahdeksan viikon määräaikaa kuudella viikolla asian monimutkaisuuden vuoksi.

1.2 Yleisen tietosuoja-asetuksen 64 artiklan 2 kohdan mukaista lausuntoa koskevan pyynnön käsiteltäväksi ottaminen

6. Yleisen tietosuoja-asetuksen 64 artiklan 2 kohdassa säädetään erityisesti, että jokainen valvontaviranomainen voi pyytää minkä tahansa yleisluonteisen tai useammassa kuin yhdessä jäsenvaltiossa vaikutuksia tuottavan asian käsittelyä tietosuojaneuvostossa lausunnon saamiseksi.

7. Tietosuojaneuvosto katsoo, että Ranskan valvontaviranomaisen esittämä pyyntö, joka koskee biometriikkaan perustuvaa todentamista tai tunnistamista varten tapahtuvan kasvontunnistusteknologian käytön yhteensopivuutta yleisen tietosuoja-asetuksen kanssa, kun tällaisen käytön nimenomaisena tarkoituksena on sujuvoittaa matkustajavirtoja lentoasemilla, liittyy ”useammassa kuin yhdessä jäsenvaltiossa vaikutuksia tuottaviin” kysymyksiin, koska – kuten pyynnössä selitetään[5] – jäsenvaltioiden lentoasemilla on parhaillaan käynnissä useita asiaan liittyviä hankkeita, ja on arvioitu, että tällainen käyttö lisääntyy lähivuosina. Eri lentoasemien ja lentoyhtiöiden tällä hetkellä testaamat mallit vaihtelevat huomattavasti eri jäsenvaltioissa, mikä voi aiheuttaa riskin siitä, että useammassa kuin yhdessä jäsenvaltiossa syntyy tietosuojan näkökulmasta erilaisia vaikutuksia.

8. Tietosuojaneuvosto katsoo myös, että Ranskan valvontaviranomaisen esittämällä pyynnöllä on merkittäviä vaikutuksia yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdassa vahvistettujen periaatteiden soveltamiseen sekä 25 artiklan nojalla rekisterinpitäjiin sovellettaviin vaatimuksiin ja 32 artiklan nojalla rekisterinpitäjiin ja henkilötietojen käsittelijöihin sovellettaviin vaatimuksiin. Näin ollen tämä pyyntö koskee yleisen tietosuoja-asetuksen 64 artiklan 2 kohdassa tarkoitettua ”yleisluontoista asiaa”, koska se liittyy säilytyksen rajoittamisen (yleisen tietosuoja-

[5] Pyyntö, s. 3.

asetuksen 5 artiklan 1 kohdan e alakohta) ja eheyden ja luottamuksellisuuden (yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohta) periaatteiden yhdenmukaiseen tulkintaan sekä sisäänrakennetun ja oletusarvoisen tietosuojan (yleisen tietosuoja-asetuksen 25 artikla) ja tietoturvallisuuden (yleisen tietosuoja-asetuksen 32 artikla) käsitteisiin, joilla varmistetaan muun muassa kyseisten säännösten johdonmukainen soveltaminen ETA:ssa.

9. Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan mahdolliset tulkintaerot jäsenvaltioiden välillä lisäisivät riskiä siitä, että lentoasemien pitäjät ja lentoyhtiöt toteuttavat kasvojentunnistushankkeita epäyhdenmukaisesti. Koska Ranskan valvontaviranomainen on osoittanut selkeästi, että näitä säännöksiä on tulkittava yhdenmukaisesti biometriikkaan perustuvaa matkustajien henkilöllisyyden todentamista tai tunnistamista palvelevan kasvojentunnistusteknologian osalta, jolla pyritään sujuvoittamaan matkustajavirtoja lentoasemilla[6], tietosuojaneuvosto katsoo, että pyyntö on perusteltu tietosuojaneuvoston työjärjestyksen 10 artiklan 3 kohdan mukaisesti.

10. Yleisen tietosuoja-asetuksen 64 artiklan 3 kohdan mukaan tietosuojaneuvosto ei anna lausuntoa, jos se on jo antanut lausunnon samasta asiasta.[7] Tietosuojaneuvosto ei ole vielä vastannut pyynnön perusteella herääviin kysymyksiin. Vaikka videolaitteita koskevissa tietosuojaneuvoston ohjeissa 3/2019[8] esitetään jo joitakin hyödyllisiä seikkoja biometristen tietojen käsittelyyn sovellettavista turvatoimenpiteistä, niissä ei käsitellä kaikkia pyynnössä esitettyihin kysymyksiin liittyviä näkökohtia. Saatavilla olevissa tietosuojaneuvoston ohjeissa, mukaan lukien videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, ei myöskään anneta erityisiä ohjeita mahdollisista seikoista, jotka olisi todennettava matkustajien tunnistamista tai heidän henkilöllisyytensä todentamista varten kerättävien biometristen tietojen keskitetyn tai hajautetun tallentamisen yhteydessä pyrittäessä sujuvoittamaan matkustajavirtoja lentoasemilla, eikä tällaisen käsittelyn yhteensopivuudesta yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa.

11. Näistä syistä tietosuojaneuvosto katsoo, että pyyntö voidaan ottaa käsiteltäväksi ja että siinä esitettyjä kysymyksiä olisi analysoitava tässä lausunnossa, joka hyväksytään yleisen tietosuoja-asetuksen 64 artiklan 2 kohdan nojalla.

2 LAUSUNNON SOVELTAMISALA JA ASIAYHTEYS

2.1 Lausunnon soveltamisala

12. Tämä lausunto koskee pyynnön mukaisesti ainoastaan sitä, onko lentoasemien pitäjien ja lentoyhtiöiden harjoittama kasvojentunnistusteknologian käyttö biometriikkaan perustuvaan matkustajien henkilöllisyyden todentamiseen tai heidän tunnistamiseensa, **kun käytön tarkoituksena on nimenomaisesti sujuvoittaa matkustajavirtoja lentoasemilla** turvatarkastuspisteissä, matkatavaroiden jättöpisteissä, koneeseen siirryttäessä ja matkustajien lounge-tilojen sisäänkäynneissä, yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa.

---

[6] Pyyntö, s. 1–3.

[7] Yleisen tietosuoja-asetuksen 64 artiklan 3 kohta ja tietosuojaneuvoston työjärjestyksen 10 artiklan 4 kohta.

[8] Euroopan tietosuojaneuvoston ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla, versio 2.0, annettu 29. tammikuuta 2020, jäljempänä ’**videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019**’.

13. **Lausunnon soveltamisalan** osalta tietosuojaneuvosto toteaa seuraavaa:

1) Henkilötietojen käsittely rajatarkastusten ja verovapaiden myymälöiden suorittamien tarkastusten yhteydessä ei kuulu tämän lausunnon soveltamisalaan, koska niitä suorittavat muut rekisterinpitäjät kuin lentoasemien pitäjät ja lentoyhtiöt.

2) Kasvontunnistusteknologian käyttö, vaikka se perustuisi jäljempänä 3.2 jaksossa kuvattuihin skenaarioihin, mihin tahansa muuhun tarkoitukseen (kuten lainvalvontaan) tai samankaltaisiin tarkoituksiin, mutta jonkin muun osapuolen suorittamana, ei kuulu tämän lausunnon soveltamisalaan.

3) Tässä lausunnossa tarkastellaan ainoastaan matkustajien henkilötietojen käsittelyä, eikä siinä käsitellä muun tyyppisiä rekisteröityjä, kuten lentoasemien pitäjien tai lentoyhtiöiden henkilöstöä.

4) Lausunnossa tarkastellaan Ranskan valvontaviranomaisen esittämää pyyntöä sen suhteen, ovatko matkustajien biometristen mallien tallennusrakenteet yhteensopivia yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa. Tältä osin lausunnossa ei tehdä kattavaa analyysiä siitä, noudattavatko asianomaiset rekisterinpitäjät ja tapauksen mukaan niiden henkilötietojen käsittelijät yleistä tietosuoja-asetusta kussakin tapauksessa. Tämä on erityisen tärkeää, kun otetaan huomioon, että nämä teknologiat lisäävät yleisen tietosuoja-asetuksen 9 artiklan mukaiseen erityisten henkilötietoryhmien käsittelyyn liittyviä riskejä. Sen vuoksi tämä lausunto ei vaikuta arviointiin siitä, onko kasvontunnistusteknologian käyttö – myös pyynnössä käsitellyllä erityisalalla – muiden yleisen tietosuoja-asetuksen säännösten mukaista, eikä tapauskohtaiseen oikeudelliseen ja tekniseen analyysiin, joka perustuu rekisterinpitäjän erityisiin suunniteltuihin käsittelytoimiin ja olosuhteisiin.

5) Tässä lausunnossa ei tarkastella lasten henkilötietojen käsittelyä eikä sillä rajoiteta tällaista käsittelyä koskevien erityisvaatimusten soveltamista.

6) Tämä lausunto ei vaikuta jäsenvaltioiden kansallisesta lainsäädännöstä johtuviin oikeudellisiin vaatimuksiin eikä biometristen tietojen käyttöä koskeviin lisärajoituksiin.[9]

7) Tässä lausunnossa esitetyt päätelmät eivät rajoita tulevaa teknologista kehitystä.

8) Lausunnossa tarkastellaan neljää skenaariota, joiden erityispiirteet kuvataan jäljempänä 3.2 jaksossa. Siinä ei käsitellä muita skenaarioita, vaikka käsittelyn tarkoitukset olisivat samat.

14. Ranskan valvontaviranomainen totesi pyynnössään, että matkustajien biometristen tietojen käsittely matkustajavirtojen sujuvoittamiseksi lentoasemilla perustuisi siihen oletukseen, että henkilöt suostuvat tällaiseen käsittelyyn, mikä mahdollisesti muodostaisi yleisen tietosuoja-asetuksen

[9] Yleisen tietosuoja-asetuksen 9 artiklan 4 kohdassa esimerkiksi säädetään, että jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön biometristen tietojen käsittelyä koskevia lisäehtoja, myös rajoituksia.

mukaisen oikeusperusteen.[10] **Sovellettavan oikeusperusteen analysointi ei kuitenkaan kuulu pyynnössä tietosuojaneuvostolle esitettyjen kysymysten piiriin, ja tästä syystä tässä lausunnossa ei tarkastella yleisen tietosuoja-asetuksen 6, 7 ja 9 artiklan mukaisen käsittelylle annetun suostumuksen pätevyyttä.**

15. Tietosuojaneuvosto toteaa kuitenkin yleisesti, että jos asianomaiset rekisterinpitäjät tukeutuisivat tähän oikeusperusteeseen, niiden olisi saatava käsittelyyn pätevä nimenomainen suostumus[11] henkilöiltä, jotka haluavat käyttää tällaisia palveluja. Tällaisen nimenomaisen suostumuksen täytyisi olla vapaaehtoisesti annettu, yksilöity ja tietoinen[12], ja näiden edellytysten täyttyminen analysoitaisiin tapauskohtaisesti. Tämä tarkoittaa muun muassa seuraavaa:

    1) Henkilöiden olisi voitava helposti peruuttaa tällainen suostumus milloin tahansa ilman, että siitä aiheutuu heille minkäänlaista haittaa.[13]

    2) Jotta suostumus voidaan antaa vapaaehtoisesti, tällainen biometriikkaan perustuvien teknologioiden käyttö voi tapahtua vain vapaaehtoiselta pohjalta, koska henkilöiden olisi voitava valita vapaasti, käyttävätkö he näitä palveluja vai eivät, ilman että siitä aiheutuu haittaa (esimerkiksi huomattavasti pidempiä viivästyksiä sellaisille matkustajille, jotka eivät anna suostumustaan[14]), kannustimia tai lisäkustannuksia tai että siitä annetaan vastineeksi lisäetuja.[15]

    3) Nimenomainen suostumus olisi pyydettävä myös henkilöiltä, joiden biometrisiä tietoja käsitellään, vaikka he eivät ole rekisteröityneet tunnistettaviksi tai todennettaviksi tällaisilla keinoilla. Toisin sanoen on olennaisen tärkeää, että niiden henkilöiden kasvoja, jotka eivät ole antaneet nimenomaista suostumustaan aiottua tarkoitusta varten suoritettavaan kasvojentunnistukseen, ei skannata kameroilla. Tämä voidaan saada aikaan esimerkiksi osoittamalla tietyt jonotuskaistat kasvojentunnistukseen, huolehtimalla asianmukaisista opasteista ja erottamalla fyysisesti muiden kuin biometristen tarkastusten kaistat, jotta tällaiset kaistat voidaan tunnistaa selkeästi.

    4) Yleisen tietosuoja-asetuksen 5 artiklassa vahvistettuja käsittelyperiaatteita, jotka koskevat tarpeellisuutta ja oikeasuhteisuutta, sovelletaan silloinkin, kun henkilöt ovat antaneet nimenomaisen suostumuksensa biometristen tietojensa käyttöön, sanotun

[10] Pyyntö, liite I.

[11] Yleisen tietosuoja-asetuksen 4 artiklan 14 kohdan ja 9 artiklan 1 kohdan sekä 9 artiklan 2 kohdan a alakohdan mukaan biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten on kielletty, ellei rekisteröity ole antanut nimenomaista suostumustaan näiden henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten, paitsi jos unionin tai jäsenvaltion lainsäädännössä säädetään, että yleisen tietosuoja-asetuksen 9 artiklan 1 kohdassa tarkoitettua kieltoa ei voida kumota rekisteröidyn suostumuksella. Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 51, 52 ja 53 kappale.

[12] Yleisen tietosuoja-asetuksen 4 artiklan 11 kohta ja 7 artikla.

[13] Yleisen tietosuoja-asetuksen 7 artiklan 4 kohta sekä johdanto-osan 50 kappale.

[14] Tähän voi sisältyä esimerkiksi sellaisen järjestelmän suunnitteleminen, jolla vältetään niihin matkustajiin kohdistuva sosiaalinen paine, jotka eivät halua antaa suostumustaan, estämällä se, että matkustajan valinta vaikuttaisi kielteisesti muihin matkustajiin.

[15] Asetuksen 2016/679 mukaista suostumusta koskevat tietosuojaneuvoston suuntaviivat 05/2020, versio 1.1, hyväksytty 4. toukokuuta 2020, jäljempänä '**suostumusta koskevat tietosuojaneuvoston suuntaviivat 05/2020**', 46 ja 48 kohta.

kuitenkaan rajoittamatta sitä, olisiko suostumus tällaiseen käsittelyyn sovellettava oikeusperuste.[16]

16. Pyynnössä täsmennetään[17], että lentoasemien pitäjät toimisivat rekisterinpitäjinä lentoasemien turvatarkastuspisteissä tapahtuvan käsittelyn osalta, kun taas lentoyhtiöt toimisivat rekisterinpitäjinä matkatavaroiden jättöpisteissä, koneeseen siirtymisen yhteydessä ja matkustajien lounge-tilojen sisäänkäynneillä tapahtuvan käsittelyn osalta. Näin ollen tietosuojaneuvosto toteaa, että pyynnössä kuvattuun käsittelyyn saattaa osallistua eri toimijoita, eikä se ole arvioinut (yhteis)rekisterinpitäjän ja/tai henkilötietojen käsittelijän roolien soveltamista jäljempänä tämän lausunnon 3.2 jaksossa kuvatuissa skenaarioissa. Kussakin tapauksessa osallistuvat toimijat on yksilöitävä ja niiden vastuualueet on jaettava selkeästi, jotta yleisen tietosuoja-asetuksen vaatimukset täyttyvät[18].

17. Lisäksi tietosuojaneuvosto toteaa, että EU:ssa ei ole tällä hetkellä yhtenäistä oikeudellista vaatimusta, jonka mukaan lentoasemien pitäjien ja lentoyhtiöiden olisi tunnistettava matkustajat ja todennettava, että matkustajan tarkastuskortissa oleva nimi vastaa heidän henkilöllisyystodistuksessaan olevaa nimeä kaikissa edellä mainituissa tarkastuspisteissä.[19] Näin ollen kaikkiin tällaisiin vaatimuksiin sovelletaan kansallista lainsäädäntöä, joka voi vaihdella eri jäsenvaltioissa. Joissakin jäsenvaltioissa tällaista todentamista saatetaan edellyttää joissakin tarkastuspisteissä (esimerkiksi matkatavaroiden jättöpisteissä tai siirryttäessä koneeseen), kun taas toisissa jäsenvaltioissa tällaisia tarkastuksia ei tällä hetkellä vaadita.[20] Matkustajien henkilöllisyyden todentamista koskevien oikeudellisten velvoitteiden olemassaolo vaikuttaa suoraan eri lentoasemien käytäntöihin.

18. Näin ollen tällaisissa tilanteissa, **joissa ei edellytetä matkustajien henkilöllisyyden todentamista virallisella henkilöllisyystodistuksella, biometristä todentamista ei pitäisi suorittaa, sillä tämä johtaisi tietojen liialliseen käsittelyyn, koska se edellyttäisi useampien tietojen käsittelyä kuin nykytilanteessa ja ylittäisi sen, mikä on tarpeen kyseessä olevaa tarkoitusta varten, ja olisi vastoin yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohdassa vahvistettua tietojen minimoinnin periaatetta.** Tämä olisi otettava huomioon tarkasteltaessa kaikkia jäljempänä tämän lausunnon 3.2 jaksossa kuvattuja skenaarioita.

2.2 Keskeiset käsitteet

[16] Ks. edellinen alaviite, 5 kohta.
[17] Pyyntö, liite I.
[18] Yleisen tietosuoja-asetuksen 4 artiklan 7 ja 8 kohdan, 5 artiklan 2 kohdan, 24, 26, 28 ja 29 artiklan mukaisesti. Ks. myös tietosuojaneuvoston suuntaviivat 07/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuoja-asetuksessa, versio 2.1, hyväksytty 7. heinäkuuta 2021.
[19] Asiaa koskeva EU:n tason säädös on komission täytäntöönpanoasetus (EY) N:o 2015/1998, annettu 5 päivänä marraskuuta 2015, yksityiskohtaisista toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöön panemiseksi. Tässä asetuksessa ei kuitenkaan käsitellä virallisten henkilöllisyystodistusten tarkastuksia lentoasemien tarkastuspisteissä, ja jäsenvaltioilla on harkintavalta säännellä tällaisia tarkastuksia kansallisella tasolla.
[20] Tämä tarkoittaa, että tällä hetkellä joko ei suoriteta mitään tarkastusta tai tarkastetaan vain, että henkilöllä on tarkastuskortti. Esimerkiksi Tanskan, Suomen, Norjan ja Ruotsin kansalaisten vapauttamisesta velvollisuudesta omata passi sekä oleskelulupa muussa pohjoismaassa kuin kotimaassa oleskellessaan 22 päivänä toukokuuta 1954 tehdyn pöytäkirjan perusteella Norjan, Tanskan, Suomen ja Ruotsin kansalaiset on 1. heinäkuuta 1954 alkaen vapautettu velvollisuudesta omata passi tai muu matkahenkilöllisyystodistus matkustaessaan näiden maiden välillä.

19. Jotta tiedot voitaisiin katsoa yleisen tietosuoja-asetuksen 4 artiklan 14 kohdan mukaisiksi biometrisiksi tiedoiksi[21], käsittelemättömien tietojen, kuten luonnollisen henkilön fyysisten, fysiologisten tai käyttäytymisen ominaisuuksien, käsittelystä on seurattava näiden ominaisuuksien mittaamista.[22]

20. Käyttämällä kuvaa henkilön kasvoista (valokuvaa tai videota), jota kutsutaan biometriseksi ”**näytteeksi**”, voidaan luoda digitaalinen esitys näiden kasvojen erottavista ominaispiirteistä (tätä kutsutaan ”**malliksi**”).[23] Lisäksi tietosuojaneuvosto muistuttaa, että ”[b]iometrinen malli on digitaalinen esitys yksilöllisistä ominaisuuksista, jotka on poimittu biometrisestä näytteestä ja jotka voidaan tallentaa biometriseen tietokantaan”[24], ja se mahdollistaa tai vahvistaa henkilön yksilöllisen tunnistamisen. Lisäksi ”[t]ämän mallin on tarkoitus olla yksilöllinen ja henkilökohtainen, ja se on lähtökohtaisesti pysyvä.”[25] Yleensä vertailuprosessissa, jonka tarkoituksena on tunnistaa henkilö tai todentaa tämän henkilöllisyys kasvojentunnistuksen avulla, tarkastuspisteeseen saapuvan henkilön biometristä mallia verrataan tallennettuihin malleihin joko vastaavan mallin todentamiseksi tai sen löytämiseksi tietokannasta.[26]

21. Kasvontunnistusteknologialla voidaan suorittaa kaksi erillistä toimintoa: henkilöllisyyden todentaminen[27] ja henkilön tunnistaminen[28]. Vaikka nämä toiminnot ovat erillisiä, ne molemmat perustuvat tunnistettuun tai tunnistettavissa olevaan henkilöön liittyvien biometristen tietojen käsittelyyn[29] ja ovat siten yleisen tietosuoja-asetuksen 9 artiklan mukaista erityisten henkilötietoryhmien käsittelyä[30].

22. Todennuksessa ja tunnistuksessa on kyse seuraavasta:

---

[21] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 51, 52 ja 53 kappale.
[22] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 74 kohta.
[23] Tietosuojaneuvoston ohjeet 5/2022 kasvojentunnistusteknologian käytöstä lainvalvonnan alalla, versio 2.0, hyväksytty 26. huhtikuuta 2023, jäljempänä ’**kasvojentunnistusta lainvalvonnassa koskevat tietosuojaneuvoston ohjeet 5/2022**’, 7 ja 8 kohta.
[24] Ks. edellinen alaviite, 9 kohta.
[25] Ks. edellinen alaviite.
[26] Kasvojentunnistusta lainvalvonnassa koskevat tietosuojaneuvoston ohjeet 5/2022, 10–11 kohta; ks. myös kansainvälinen standardi ISO/IEC 2382-37, 2022-03,
saatavilla osoitteessa https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [sivustolla käyty viimeksi 23.5.2024], jäljempänä ’**standardi ISO/IEC 2382-37**’.
[27] Tietosuojaneuvosto toteaa, että myös tekoälyä koskevista yhdenmukaistetuista säännöistä annettavan Euroopan parlamentin ja neuvoston asetuksen (tekoälysäädös) (ei vielä julkaistu virallisessa lehdessä) 3 artiklan 36 alakohdan mukaan ”biometrisellä todennuksella” tarkoitetaan ”luonnollisten henkilöiden henkilöllisyyden automaattista yksi yhteen -todentamista, tunnistautuminen mukaan lukien, vertaamalla näiden biometrisiä tietoja aiemmin annettuihin biometrisiin tietoihin” (ks. Euroopan parlamentin lainsäädäntöpäätöslauselma 13. maaliskuuta 2024 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen unionin säädösten muuttamisesta (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).
[28] Tekoälysäädöksen 3 artiklan 35 alakohdan mukaan ”biometrisellä tunnistuksella” tarkoitetaan ”ihmisen fyysisten, fysiologisten, käyttäytymiseen liittyvien tai psykologisten ominaisuuksien automaattista tunnistamista luonnollisen henkilön henkilöllisyyden toteamiseksi vertaamalla kyseisen henkilön biometrisiä tietoja tietokantaan tallennettuihin toisten yksilöiden biometrisiin tietoihin”.
[29] Standardi ISO/IEC 2382-37.
[30] Yleisen tietosuoja-asetuksen 4 artiklan 14 kohta ja kasvojentunnistusta lainvalvonnassa koskevat tietosuojaneuvoston ohjeet 5/2022, 12 kohta.

Todentamisella pyritään vahvistamaan biometrinen tieto vertailun avulla. Tätä kutsutaan myös yksi yhteen -todennukseksi.

Tunnistamisella pyritään hakemaan rekisteröityjen biometristen tietojen tietokannasta yksittäisen henkilön tunnisteita. Tätä kutsutaan myös yksi moneen -tunnistukseksi.

23. Molemmissa tapauksissa (eli tunnistuksessa ja todennuksessa) kasvojentunnistustekniikat perustuvat arvioituun vastaavuuteen mallien, eli verrattavan mallin ja vertailumallin tai -mallien, välillä. Tästä näkökulmasta katsottuna ne perustuvat todennäköisyyteen: vertailussa päätellään suurempi tai pienempi todennäköisyys sille, että henkilö on tosiaan kyseinen tunnistettava tai todennettava henkilö. Jos tämä todennäköisyys ylittää järjestelmässä tietyn kynnysarvon, jonka järjestelmän käyttäjä tai kehittäjä on määritellyt, järjestelmä olettaa, että mallit vastaavat toisiaan, eli syntyy tunnistettava tai todennettava osuma.[31]

[31] Kasvojentunnistusta lainvalvonnassa koskevat tietosuojaneuvoston ohjeet 5/2022, 11 kohta. Katso myös standardi ISO/IEC 2382-37.

3 PYYNNÖN PERUSTEET

3.1 Yleisiä huomioita

24. Tässä jaksossa analysoidaan edellä 4 kohdassa esitettyjä kysymyksiä. Tässä yhteydessä tietosuojaneuvosto analysoi kysymyksen 1 osalta yhteensopivuutta yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan sekä 25 ja 32 artiklan kanssa ja kysymyksen 2 osalta yhteensopivuutta yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa.

25. Tätä varten tietosuojaneuvosto analysoi neljää eri skenaariota[32], joiden erityispiirteet kuvataan jäljempänä 3.2 jaksossa.

26. Tietosuojaneuvosto muistuttaa alustavana huomautuksena, että biometristen tietojen ja erityisesti kasvojentunnistusteknologian käyttö lisää rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä. Käsittely koskee ensinnäkin biometrisiä tietoja, joille myönnetään yleisen tietosuoja-asetuksen 9 artiklassa erityinen suoja. Biometriset tiedot muuttavat peruuttamattomasti ruumiin ja henkilöllisyyden suhdetta, sillä biometristen tietojen avulla ihmisruumiin piirteistä tulee ”koneellisesti luettavia” mahdollista myöhempää käyttöä varten.[33] Kasvontunnistusteknologian käyttö voi lisäksi aiheuttaa vääriin negatiivisiin tuloksiin, vääristymiin ja syrjintään liittyviä riskejä[34], ja biometristen tietojen väärinkäytön mahdollisuus voi aiheuttaa henkilöiden kannalta vakavia seurauksia, kuten henkilöllisyyspetoksia tai toisena henkilönä esiintymistä[35]. On myös huomattava, että jos kasvojentunnistus tehdään etänä ja ilman rekisteröidyn aktiivista osallistumista, henkilöt saattavat olla vielä vähemmän tietoisia tällaisesta käsittelystä ja siihen liittyvistä riskeistä. Lisäksi on tärkeää korostaa, että ominaisuuksia, joihin biometriset tiedot perustuvat, voidaan yleensä pitää pysyvinä, ja niitä olisi käsiteltävä peruuttamattomina ominaisuuksina erityisesti kasvojentunnistuksen yhteydessä.[36]

27. Vaikka tällaisten teknologioiden käyttöä pidettäisiin erityisen tehokkaana, rekisterinpitäjien olisi edellä esitetyn perusteella ennen niiden käyttämistä arvioitava vaikutuksia rekisteröityjen perusoikeuksiin ja -vapauksiin ja pohdittava, voitaisiinko käsittelyn laillinen tarkoitus saavuttaa yksityisyyteen vähemmän puuttuvilla keinoilla.[37]

---

[32] Tietosuojaneuvoston analysoimat neljä skenaariota perustuvat pyynnön liitteessä I esitettyihin käyttötapauksiin. Ranskan valvontaviranomainen on selventänyt, että pyynnön liitteessä I esitetyt käyttötapaukset ovat tiettyyn skenaarioon liittyviä havainnollistavia esimerkkejä täytäntöönpanosta.

[33] Tietosuojatyöryhmän lausunto 3/2012 biometristen tekniikoiden kehityksestä, annettu 27. huhtikuuta 2012, WP193, jäljempänä ’**biometrisiä tekniikkoja koskeva tietosuojatyöryhmän lausunto 3/2012**’, s. 4. On huomattava, että tässä lausunnossa viitataan yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annettuun direktiiviin 95/46/EY, jäljempänä ’tietosuojadirektiivi’. Yleisessä tietosuoja-asetuksessa on laajennettu erityisten tietoryhmien soveltamisalaa, ja toisin kuin tietosuojadirektiivissä, yleisessä tietosuoja-asetuksessa säädetään, että biometriset tiedot ovat erityisiä tietoryhmiä (yleisen tietosuoja-asetuksen 9 artikla).

[34] Yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn Euroopan neuvoston yleissopimuksen neuvoa-antavan komitean antamat kasvojentunnistusta koskevat suuntaviivat, kesäkuu 2021, s. 15; ks. myös kasvojentunnistusta lainvalvonnassa koskevat tietosuojaneuvoston ohjeet 5/2022, 27 kohta.

[35] Biometrisiä tekniikkoja koskeva tietosuojatyöryhmän lausunto 3/2012, s. 29.

[36] Kasvojentunnistusta lainvalvonnassa koskevat tietosuojaneuvoston ohjeet 5/2022, 104 kohta.

[37] Yleisen tietosuoja-asetuksen johdanto-osan 39 kappale; ks. myös videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 73 kohta.

28. Tietosuojaneuvosto muistuttaa myös, että oikeus henkilötietojen suojaan ei ole absoluuttinen oikeus ja että sen on suhteellisuusperiaatteen mukaisesti oltava oikeassa suhteessa muihin perusoikeuskirjassa suojattuihin perusoikeuksiin.[38]

29. Yleisen tietosuoja-asetuksen 25 artiklan 1 kohdassa viitataan yleisen tietosuoja-asetuksen 5 artiklassa lueteltuihin tietosuojaperiaatteisiin[39] ja edellytetään, että ne pannaan täytäntöön ”tehokkaasti” sisäänrakennetun tietosuojan avulla.[40] Tähän sisältyy nimenomaisesti yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohdan mukainen tietojen minimoinnin periaate[41], jonka mukaan henkilötietojen on oltava ”asianmukaisia ja olennaisia ja ne on rajattava siihen, mikä on tarpeen niitä tarkoituksia varten, joita varten niitä käsitellään, mikä on ilmaus mainitusta suhteellisuusperiaatteesta”[42]. Lisäksi yleisen tietosuoja-asetuksen 25 artiklan 2 kohdassa täsmennetään oletusarvoista tietojen minimointia koskevaa velvollisuutta toteamalla, että se koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa.[43]

30. Yleisen tietosuoja-asetuksen 25 artiklassa ei kuitenkaan edellytetä minkään tiettyjen teknisten ja organisatoristen toimenpiteiden toteuttamista, vaan sitä, että valittujen toimenpiteiden ja suojatoimien olisi liityttävä erityisesti käsittelyn asiayhteyteen ja sen aiheuttamiin rekisteröidyn oikeuksiin ja vapauksiin kohdistuviin riskeihin.[44] Vastaavasti käsittelyn turvallisuutta koskevassa yleisen tietosuoja-asetuksen 32 artiklassa edellytetään, että rekisterinpitäjät ja henkilötietojen

---

[38] Yleisen tietosuoja-asetuksen johdanto-osan 4 kappale. Ks. tältä osin myös unionin tuomioistuimen tuomio 22.6.2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504, jäljempänä ’asiassa C-439/19, Latvijas Republikas Saeima, annettu tuomio’, 98, 110 ja 113 kohta. Lisäksi suhteellisuusperiaate, joka kuuluu unionin oikeuden yleisiin periaatteisiin edellyttää, että kyseessä oleva tavoite on toteutettavissa unionin toimessa säädettyjen keinojen avulla ja että näillä keinoilla ei ylitetä sitä, mikä on tarpeen tämän tavoitteen saavuttamiseksi (ks. unionin tuomioistuimen tuomio 9.11.2010, Volker und Markus Schecke ja Eifert, C-92/09 ja C-93/09, ECLI:EU:C:2010:662, jäljempänä ’asioissa C-92/09 ja C-93/09, Volker ja Schecke, annettu tuomio’, 74 kohta oikeuskäytäntöviittauksineen.

[39] Ks. tietosuojaneuvoston ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, versio 2.0, hyväksytty 20. lokakuuta 2020, jäljempänä ’**tietosuojaneuvoston ohjeet 4/2019 sisäänrakennetusta ja oletusarvoisesta tietosuojasta**’, 11 kohta.

[40] Yleisen tietosuoja-asetuksen 25 artiklan 1 kohdassa säädetään seuraavaa: ”Ottaen huomioon uusimman teknologian, toteuttamiskustannukset ja käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille rekisterinpitäjän on sekä käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten tietojen pseudonymisointi, tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten, jotta tarvittavat suojatoimet saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi tämän asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin.” Ks. myös Euroopan tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 13 kohta.

[41] Yleisen tietosuoja-asetuksen johdanto-osan 39 kappaleessa todetaan vastaavasti, että henkilötietoja olisi käsiteltävä vain jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.

[42] Asiassa C-439/19, Latvijas Republikas Saeima, annettu tuomio, 98 kohta; unionin tuomioistuimen tuomio 11.12.2019, Asociatia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064, jäljempänä ’asiassa C-708/18, M5A-ScaraA, annettu tuomio’, 48 kohta.

[43] Tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 48 kohta.

[44] Tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 14 kohta.

käsittelijät toteuttavat luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet.

31. On tärkeää huomata, että vaikka matkustajat antaisivat nimenomaisen suostumuksensa biometristen tietojensa käyttöön matkustajavirtojen sujuvoittamiseksi lentoasemilla, yleisessä tietosuoja-asetuksessa säädettyjä käsittelyperiaatteita, jotka koskevat tarpeellisuutta ja oikeasuhteisuutta, sovelletaan edelleen ja niitä on noudatettava.[45]

32. **Tarpeellisuuden periaatteen** osalta tietosuojaneuvosto pohtii, onko ehdotettu käsittely tarpeen tavoitellun tavoitteen saavuttamiseksi ja voidaanko sama tavoite saavuttaa tehokkaasti muilla keinoilla, joilla puututaan vähemmän rekisteröidyn perusoikeuksiin ja -vapauksiin.[46] **Oikeasuhteisuuden periaatteen** osalta tietosuojaneuvosto arvioi, onko rekisteröityjen perusoikeuksiin ja -vapauksiin kohdistuva kielteinen vaikutus oikeassa suhteessa ennakoituun hyötyyn. Jos etu on suhteellisen vähäinen, vaikutus ei ehkä ole oikeasuhteinen.[47]

33. Vaikka tietosuojaneuvosto katsoisi, että jokin jäljempänä analysoiduista skenaarioista voisi täyttää yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan vaatimukset, rekisterinpitäjän on tästä huolimatta kussakin tapauksessa osoitettava tämä tosiseikoilla. Tällaisessa osoittamisessa olisi otettava huomioon vaihtoehtoiset skenaariot.

3.2 Yhteensopivuus yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa

3.2.1 Skenaario 1: rekisteröidyn biometrisen mallin säilyttäminen vain henkilön hallussa todentamista varten

34. Tässä jaksossa tarkastellaan, onko matkustajien biometrisen mallin säilyttäminen ainoastaan henkilön hallussa, esimerkiksi hänen henkilökohtaisella laitteellaan[48], joka on hänen yksinomaisessa valvonnassaan[49] todentamista varten[50], jäljempänä ’**skenaario 1**’, yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan sekä 25 ja 32 artiklan kanssa. Tässä jaksossa tarkastellaan myös skenaariota 1 koskevia asianmukaisia suojatoimia yleisen tietosuoja-asetuksen 25 ja 32 artiklan valossa.

Skenaarion kuvaus

35. Skenaariossa 1 kunkin tällaiseen käsittelyyn suostumuksensa antaneen matkustajan rekisteröity biometrinen malli säilytetään vain kyseisen henkilön hallussa, esimerkiksi kunkin matkustajan henkilökohtaisella laitteella, joka on hänen yksinomaisessa valvonnassaan. Matkustajien henkilöllisyys todennetaan (yksi yhteen -vertailu), kun he kulkevat lentoaseman tiettyjen tarkastuspisteiden läpi.

---

[45] Asetuksen 2016/679 mukaista suostumusta koskevat tietosuojaneuvoston suuntaviivat 05/2020, 5 kohta.
[46] Asiassa C-439/19, Latvijas Republikas Saeima, annettu tuomio, 110 ja 113 kohta; unionin tuomioistuimen tuomio (suuri jaosto) 4.7.2023, Meta v. Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, 108 kohta.
[47] Asiassa C-708/18, M5A-ScaraA, annettu tuomio, 52–56 kohta, asioissa C-92/09 ja C-93/09, Volker ja Schecke, annettu tuomio, 87 kohta, ja asiassa C-439/19, Latvijas Republikas Saeima, annettu tuomio, 98, 110 ja 113 kohta. Ks. myös biometrisiä tekniikkoja koskeva tietosuojatyöryhmän lausunto 3/2012, s. 8.
[48] Vaihtoehtoisesti henkilö voisi tulostaa ja tallentaa biometrisen mallinsa paperille.
[49] Tämä ei rajoita rekisterinpitäjän yleisvastuuta käsittelystä.
[50] Pyynnön liitteessä I olevan käyttötapauksen 1 mukaisesti.

36. Rekisteröinnin tekee lentoaseman pitäjä joko etänä lentoaseman pitäjän sovelluksen avulla[51] tai lentoaseman päätelaitteilla asianmukaisella tunnistamisen varmuustasolla (esimerkiksi eIDAS-kehyksen asianmukaisella varmuustasolla[52]). Tällainen rekisteröinti koostuu biometristen mallien ja käsittelyssä tarvittavien tunnistetietojen[53] tallentamisesta matkustajan laitteelle. Rekisteröinti tapahtuu vain kerran ja on voimassa tietyn ajan (esimerkiksi matkustajien passin voimassaoloajan). Lentoaseman pitäjä ei säilytä matkustajien tunnistetietoja eikä heidän biometrisiä tietojaan rekisteröinnin jälkeen.

37. Erityisesti säilyttämisen osalta voidaan todeta, että matkustajan tunnistetiedot ja biometrinen malli tallennetaan paikallisesti kunkin matkustajan laitteelle (esimerkiksi lentoaseman pitäjän mobiilisovellukseen tai verkkolompakkosovellukseen). Tämän jälkeen laitteen avulla voidaan lähettää tai kysellä matkustajien tunnistetietoja ja biometrisiä malleja, mahdollisesti myös lentotietoja ja/tai tarkastuskortteja. Nämä tiedot voidaan salata esimerkiksi vain lentoaseman pitäjän hallussa olevalla avaimella. Avain voidaan koodata QR-koodiksi, joka puolestaan voidaan joko tulostaa paperille tai näyttää matkustajan laitteen näytöllä. Tässä tapauksessa matkustaja näyttäisi QR-koodin lentoasemalla erityiselle tarkastuslaitteelle, jossa on QR-koodinlukija ja kamera.

38. Turvallisuuden osalta QR-koodien salaus puretaan vertailun aikana lentoaseman pitäjän hallussa olevalla avaimella, joka on ainoa avain, jolla QR-koodien salaus pystytään purkamaan. Matkustajien biometrisiä tietoja säilytetään vain hyvin lyhyen ajan ja ne poistetaan vertailun päätyttyä. On huomattava, että säilytystä koskevat turvatoimet riippuvat osittain matkustajan laitteen turvallisuudesta.

Tietosuojaneuvoston arvio

39. Skenaariossa 1 kuvataan teknisiä ja organisatorisia toimenpiteitä, joiden tarkoituksena on varmistaa rekisteröityihin kohdistuvia riskejä vastaava turvallisuustaso yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan mukaisesti. Matkustajien henkilöllisyys todennetaan (yksi yhteen -vertailu), kun he kulkevat lentoaseman tiettyjen tarkastuspisteiden läpi. Tässä skenaariossa pääasiallinen vertailu suoritetaan valvotussa ympäristössä[54], jossa matkustajat osallistuvat vertailuun aktiivisesti ja voivat hallita paremmin tietojaan. Skenaariossa tarkastettaisiin vain sellaiset matkustajat, jotka ovat antaneet suostumuksensa tällaiseen käsittelyyn, ja koska tarkastus suoritettaisiin erityisillä tarkastuslaitteilla, biometrisiä tietoja ei kerättäisi muista matkustajista, jotka

[51] Tietosuojaneuvosto huomauttaa, että tällaisen rekisteröinnin suorittamiseksi voitaisiin tulevaisuudessa harkita vaihtoehtoisia tapoja ja että rekisteröinti voitaisiin mahdollisesti suorittaa ilman erityistä lentoaseman pitäjän sovellusta esimerkiksi olemalla vuorovaikutuksessa käyttäjän digitaalisen lompakon kanssa.

[52] Sähköistä tunnistamista ja sähköisiin transaktioihin liittyviä luottamuspalveluja koskeva kehys, jäljempänä **eIDAS-kehys**, joka perustuu asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta 11 päivänä huhtikuuta 2024 annettuun Euroopan parlamentin ja neuvoston asetukseen (EU) 2024/1183.

[53] Tässä lausunnossa tunnistetiedoilla tarkoitetaan tietoja, kuten sukunimeä, etunimeä ja syntymäaikaa, joiden on varmennettu pitävän paikkansa henkilöllisyystodistuksen tai passin osalta.

[54] ”Valvomattomalla ympäristöllä” tarkoitetaan kasvontunnistuksen käyttöä tunnistukseen ilman rekisteröityjen aktiivista osallistumista siten, että jokaisten valvonta-alueelle tulevien henkilöiden kasvojen mallia verrataan tietokantaan tallennettuihin kattavaan väestömäärään perustuviin malleihin (ks. tietosuojaneuvoston ohjeet 5/2022 kasvontunnistuksesta lainvalvonnassa, 17 kohta).

eivät ole antaneet suostumustaan tällaiseen käsittelyyn. Lisäksi suostumuksen antaneilla matkustajilla on mahdollisuus lopettaa käsittely milloin tahansa poistamalla tiedot laitteestaan.

40. Jos kasvontunnistus perustuu ainoastaan henkilön hallussa säilytettävään biometriseen malliin, joka voi esimerkiksi olla matkustajan yksinomaisessa valvonnassa olevalla henkilökohtaisella laitteella, ja sitä käytetään todentamiseen tietyissä tarkastuspisteissä erityisen käyttöliittymän avulla, sen käyttö aiheuttaa tietyissä olosuhteissa vähemmän riskejä kuin biometristen tietojen käyttö, jossa tiedot tallennetaan keskitettyyn tietokantaan.[55] Tällaisella paikallisella säilyttämisellä ja asianmukaisilla suojatoimilla[56] vähennetään henkilötietojen tietoturvaloukkausten vakavuutta keskitettyyn säilyttämiseen verrattuna tietoturvaloukkausten kohteiksi joutuneiden henkilöiden määrän osalta ja varmistetaan, että biometriseen malliin pääsy edellyttää rekisteröidyn aktiivista osallistumista.

41. Lisäksi vertailu voitaisiin tehdä paikallisesti lentoasemalla vertaamalla esimerkiksi QR-koodin sisältämää biometristä mallia tarkastuslaitteen kameralla otetun biometrisen näytteen perusteella laskettuun malliin. Kulloisenkin tarkastuksen suorittava rekisterinpitäjä saisi tietoonsa vain osuman ja voisi käyttää vain sitä (rekisterinpitäjä voisi olla joko lentoaseman pitäjä tai lentoyhtiö sen mukaan, tehdäänkö tarkastus lentoaseman turvatarkastuspisteissä, matkatavaroiden jättöpisteessä, koneeseen siirtymisen yhteydessä ja/vai matkustajien lounge-tilan sisäänkäynnillä). Lisäksi se, että vertailun edellyttämien tietojen (esimerkiksi QR-koodin) on oltava henkilön antamia, toimii toisena todentamisen turvallisuutta vahvistavana tekijänä.[57]

42. Yleisen tietosuoja-asetuksen 25 artiklan mukaisuuden osalta ja erityisesti tietojen minimointia koskevan vaatimuksen noudattamiseksi olisi varmistettava, että käsittely on tarpeellisuuden periaatteen mukaista. Skenaariossa 1 valittujen toimenpiteiden voidaan katsoa täyttäneen tarpeellisuuden periaatteen tavoiteltuun tarkoitukseen (eli matkustajavirran sujuvoittamiseen) nähden, jos rekisterinpitäjä voi käsittelyn olosuhteista riippuen osoittaa, ettei ole olemassa yksityisyyteen vähemmän puuttuvia vaihtoehtoisia ratkaisuja, joilla sama tavoite voitaisiin saavuttaa yhtä tehokkaasti. Rekisterinpitäjä saattaa esimerkiksi pystyä osoittamaan, että vaikka matkustajien on esitettävä laitteensa, skenaario 1 nopeuttaa todentamisprosessia nykytilanteeseen verrattuna, jossa ihminen tarkastaa, vastaako tarkastuskortissa oleva nimi matkustajan henkilöllisyystodistusta.[58] Tätä ei voitaisi osoittaa, jos matkustajien henkilöllisyyttä ei tällä hetkellä tarkasteta virallisen henkilöllisyystodistuksen perusteella (ks. edellä 18 kohta).

43. Lisäksi lentoaseman pitäjä ei säilytä biometrisiä malleja rekisteröinnin jälkeen, ja tarkastuksen suorittava rekisterinpitäjä säilyttää biometrisia tietoja hyvin lyhyen ajan, koska tällaiset tiedot poistetaan heti, kun vertailu on saatu päätökseen. Näin ollen skenaariossa 1 valitut toimenpiteet näyttävät rajoittavan henkilötietojen käsittelyn laajuutta ja säilytysaikaa.

44. Oikeasuhteisuuden periaatteen osalta tällaisesta käsittelystä johtuvaa yksityisyyteen puuttumista voidaan tasapainottaa matkustajien aktiivisella osallistumisella, koska heidän biometriset tietonsa säilytettäisiin ainoastaan heidän hallussaan. Kun lisäksi otetaan huomioon edellä kuvatut

[55] Kasvojentunnistusta lainvalvonnassa koskevat tietosuojaneuvoston ohjeet 5/2022, 17 kohta.
[56] Suojatoimia käsitellään jäljempänä 46 kohdassa.
[57] Tämä vähentää esimerkiksi toisena henkilönä esiintymisen riskiä. Ks. myös jäljempänä esitetty suojatoimi C.1.2.
[58] Voidaan myös väittää, että biometrinen tarkastus saattaa olla vähemmän virhealtis kuin ihmisen suorittama tarkastus.

toimenpiteet ja oletetaan, että rekisterinpitäjä toteuttaa kyseisen erityisen käsittelyn edellyttämät asianmukaiset suojatoimet, toteuttamalla asianmukaiset toimenpiteet voitaisiin varmistaa riskiä vastaava turvallisuustaso. Tällöin rekisteröityjen perusoikeuksiin ja -vapauksiin kohdistuvan kielteisen vaikutuksen voitaisiin katsoa olevan oikeassa suhteessa ennakoituun hyötyyn.

45. Näin ollen tietosuojaneuvosto katsoo edellä esitetyn perusteella kysymyksen 1.1 osalta, että tällaisen käsittelyn **voitaisiin periaatteessa katsoa olevan yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan, 25 artiklan ja 32 artiklan kanssa, mikäli toteutetaan asianmukaiset suojatoimet**.

Asianmukaiset suojatoimet

46. Tämäntyyppisessä skenaariossa tietosuojaneuvosto katsoo kysymyksen 1.2 osalta, että olisi toteutettava ainakin jäljempänä esitetyt suojatoimet. Muita kuin tässä lausunnossa kuvattuja suojatoimia voitaisiin käyttää samojen turvallisuus- ja tietosuojatavoitteiden saavuttamiseksi, ja ne voivat olla laillisia, mikäli niillä varmistetaan sovellettavan oikeudellisen kehyksen noudattaminen.

47. Huomautus: Tämä on yleistasoinen ja viitteellinen yleiskatsaus mahdollisista asianmukaisista suojatoimista, jotka rekisterinpitäjän olisi toteutettava skenaarion 1 kaltaisessa ratkaisussa. Niiden asianmukaisuutta yleisen tietosuoja-asetuksen 25 ja 32 artiklan nojalla on analysoitava tapauskohtaisesti. Kaikkien rekisterinpitäjien on varmistettava, että ne suorittavat oman tietosuojaa koskevan vaikutustenarvioinnin[59], ja niiden kulloisetkin ratkaisut saattavat edellyttää lisätoimenpiteitä, joita ei käsitellä tässä lausunnossa.

A. Yleistä

A.1 Tietojenkäsittelyn vaikutusten arviointi

A.1.1 Suoritetaan tietosuojaa koskeva vaikutustenarviointi yleisen tietosuoja-asetuksen 35 artiklan vaatimusten mukaisesti aina, kun rekisterinpitäjä suunnittelee uutta käsittelytoimea, johon liittyy todennäköisesti suuren riskin aiheuttavaa tietojen käsittelyä. Skenaariossa 1 näin todennäköisesti on, koska siinä käsitellään biometrisiä tietoja laajamittaisesti.[60] Arvioidaan, onko kasvojentunnistusjärjestelmän käyttöönotto tarkoituksenmukaista, mukaan lukien sen tarpeellisuus ja oikeasuhteisuus tavoiteltuihin tarkoituksiin nähden[61], suunnittelun varhaisessa vaiheessa ja tarkistetaan sitä koko tuotekehityksen elinkaaren ajan.

A.1.2 Kuullaan asianomaista valvontaviranomaista, jos käsittely aiheuttaa edelleen suuren riskin huolimatta toimenpiteistä, joita rekisterinpitäjä on toteuttanut riskin pienentämiseksi.[62]

[59] Yleisen tietosuoja-asetuksen 35 artikla.
[60] Yleisen tietosuoja-asetuksen 35 artiklan 3 kohta ja tietosuojatyöryhmän ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” 13. lokakuuta 2017 annetussa asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”, WP 248 rev.01 (tietosuojaneuvoston hyväksymä asiakirja).
[61] Yleisen tietosuoja-asetuksen 35 artiklan 7 kohdan b alakohta.
[62] Yleisen tietosuoja-asetuksen 36 artiklan 1 kohta.

A.2 Rekisteröityjen oikeudet ja suojatoimet, jotka rekisterinpitäjät voivat toteuttaa

A.2.1 Suojatoimet, joilla ehkäistään vääriä negatiivisia tuloksia. Vähennetään ikään, sukupuoleen ja rotuun perustuvien vinoutumien riskiä arvioimalla ”säännöllisesti, toimivatko algoritmit tarkoitusten mukaisesti, ja mukauttamalla algoritmeja havaittujen vinoutumien lieventämiseksi ja käsittelyn tasapuolisuuden varmistamiseksi”[63]. Tämä voidaan saada aikaan esimerkiksi toteuttamalla ihmisen suorittamaa valvontaa ja ihmisen toteuttamia toimia, jotta voidaan lieventää mahdollisia vinoutumia ja varmistaa, että matkustajia ei leimata tai profiloida.

A.2.2 Varmistetaan, että kaikki henkilötietojen käsittely on läpinäkyvää ja että henkilöt ovat tietoisia siitä, miten heidän tietojaan käsitellään kussakin käsittelytoimessa, ja voivat valvoa sitä.[64]

A.2.3 Varmistetaan, että käytössä on toimenpiteitä käyttötarkoitussidonnaisuuden periaatteen noudattamiseksi, jotta tietoja ei käytetä muihin tarkoituksiin, kuten turvallisuuteen liittyviin tai koulutustarkoituksiin.

A.2.4 Varmistetaan asianmukaisin toimenpitein, että henkilöistä, jotka eivät anna suostumustaan kasvojentunnistukseen, ei oteta valokuvia tai videoita, vaikka niitä ei tallennettaisi eikä käsiteltäisi (tämä voidaan varmistaa esimerkiksi käyttämällä sopivaa syväterävyyttä ja kuvausaluetta, jotta vältetään kuvien ottaminen taustalla tai ympärillä olevista muista matkustajista, tai käyttämällä erityisiä selvästi merkittyjä jonoja kasvojentunnistukseen).

A.2.5 Jos sekä matkustajat, jotka antavat suostumuksen kasvontunnistukseen, että kasvontunnistuksesta kieltäytyvät matkustajat voivat käyttää samoja tarkastuslaiteita tai saattavat näkyä laitteen kuvakentässä järjestelmän ollessa poissa käytöstä, odotetaan suostumuksen antaneen matkustajan selkeää toimea ennen valokuvauksen tai videoinnin aloittamista.

A.2.6 Rekisteröidyllä on mahdollisuus milloin tahansa poistaa tietoja, jotka ovat yksinomaan hänen hallussaan (biometrinen malli[65]) mobiilisovelluksessa tai digitaalisessa lompakossa[66].

A.2.7 Tarjotaan toteuttamiskelpoisia vaihtoehtoja tai vararatkaisuja (matkustajille, jotka eivät suostu biometristen tietojensa käyttöön, matkustajille, jotka eivät pysty käyttämään tällaisia

[63] Tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, alaviite 60, 70 kohta.
[64] Tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 68 kohta, ja yleisen tietosuoja-asetuksen johdanto-osan 7 kappale.
[65] Skenaarion 1 suojatoimissa olevat viittaukset biometriseen malliin vastaavat viittauksia avaimeen/salasanaan skenaariossa 2.
[66] On huomattava, että tämä suojakeino koskee vain skenaariota 1.

ratkaisuja, tai matkustajille, jotka kärsivät virheellisistä hylkäämisistä), jotta varmistetaan myös, että matkustajille, jotka eivät anna suostumustaan, ei aiheudu haittaa[67].

A.2.8 Jos käytetään sovellusta, se on suunniteltava ja konfiguroitava huolellisesti, jotta vältetään tarpeettomien tietojen kerääminen ja tietoja muihin tarkoituksiin keräävien kolmansien osapuolten ohjelmistokehityspakettien käyttö.

A.3 Osoitusvelvollisuus

A.3.1 Arvioidaan, onko olemassa asiaankuuluvia käytännesääntöjä tai sertifiointimekanismeja, joiden avulla voidaan osoittaa, että käsittely on turvallista, kuten yleisen tietosuoja-asetuksen 32 artiklassa säädetään.[68] Tarkistetaan toimenpiteiden asianmukaisuus kyseessä olevan käsittelyn osalta. Rekisterinpitäjien ryhmiä edustavien yhdistysten tai muiden elimien tunnustamat standardit[69], parhaat käytännöt ja käytännesäännöt voivat olla avuksi asianmukaisten toimenpiteiden määrittämisessä.

A.3.2 Varmistetaan, että käyttäjän laitteelle tehdään perustason turvallisuustarkastukset rekisteröintivaiheen mahdollistamiseksi, vaikka myös matkustajan on omalta osaltaan suojattava tietonsa, koska ne tallennetaan hänen laitteelleen. Esimerkkejä tällaisista teknisistä tarkastuksista on jäljempänä jaksossa C.2 ”Infrastruktuuri ja verkko”.

B. Organisaatio:

B.1 Periaatteet ja säännösten noudattaminen

B.1.1. Varmistetaan, että käytössä on sisäinen pääsynvalvonta[70], joka sisältää järjestelmänvalvojia koskevat säännöt.

B.1.2 Jos jokin käsittelyyn osallistuvista osapuolista voi tarjota kasvontunnistuspalvelua ilman tunnistetietoja tai biometrisiä tietoja tai molempia tietoja, joita muiden osapuolten täytyisi käsitellä, kielletään kyseisten tietojen kulkeminen näiden muiden osapuolten kautta. Esimerkiksi lentoyhtiön ei tarvitse teknisesti saada biometrisiä tietoja, jos se käyttää lentoaseman yhteistä infrastruktuuria, vaikka kyseinen lentoyhtiö toimisi yleisen tietosuoja-asetuksen mukaisena käsittelyn rekisterinpitäjänä.

[67] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 86 kohta.
[68] Yleisen tietosuoja-asetuksen 32 artiklan 3 kohta ja tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 10 kohta.
[69] Ks. esimerkiksi standardi ISO/IEC 2382-37.
[70] Euroopan tietosuojaneuvoston ohjeet 4/2020 sijaintitietojen ja kontaktien jäljitysvälineiden käytöstä covid-19-epidemian yhteydessä, annettu 21. huhtikuuta 2020, jäljempänä ’**tietosuojaneuvoston ohjeet 4/2020 sijaintitiedoista ja kontaktien jäljitysvälineistä**’, SEC-10, s. 19.

B.1.3 Määritetään salausta ja avaimenhallintaa koskeva käytäntö[71] esimerkiksi tunnistetietojen ja biometristen tietojen käsittelyä varten.

B.1.4 Varmistetaan yleisen tietosuoja-asetuksen V luvun noudattaminen. Varmistetaan esimerkiksi säännösten mukaiset siirrot, jos rekisterinpitäjä käyttää rekisteröintiprosessin aikana kolmannessa maassa sijaitsevaa etäpalvelua.

B.1.5 Jos käytetään henkilötietojen käsittelijöitä, varmistetaan, että henkilötietojen käsittelijää koskeva sopimus[72] on tehty yleisen tietosuoja-asetuksen 28 artiklan 3 kohdan mukaisesti.

B.1.6 Varmistetaan, että käytössä on menettelyt ihmisen suorittaman valvonnan ja ihmisen toteuttamien toimien hallitsemiseksi, erityisesti virheellisiin hylkäämisiin liittyvien ongelmien sekä teknisten tai käytettävyyttä koskevien kysymysten käsittelemistä varten.

B.2 Koulutus ja testaus

B.2.1. Varmistetaan, että henkilöstöllä on asianmukainen koulutus.

B.2.2 Otetaan käyttöön ”menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi”.[73]

B.2.3. Otetaan käyttöön prosessi, jolla varmistetaan, että matkustajan biometrisen mallin[74] käsittely todentamista varten on teknisesti tehokasta ja riittävän tarkkaa.

B.2.4. Varmistetaan, että sekä rekisteröinnin yhteydessä että tarkastuspisteessä kerätyt biometriset näytteet ovat riittävän laadukkaita luotettavan biometrisen käsittelyn suorittamiseksi.

C. Tekninen ulottuvuus:

C.1 Pääsy tietoihin

C.1.1 Toteutetaan rekisteröitymisvaiheen aikana suojatoimia, joilla varmistetaan, että rekisteröintiprosessin esilatauksessa käytetään todennettua henkilöllisyyttä. Käyttäjien henkilöllisyyden monivaiheisen todennuksen arvioinnin vahvistamiseksi voidaan esimerkiksi ottaa käyttöön erilaisia vaiheita salasanalla suojatuista kertakäyttöisistä linkeistä, joilla sovellus aktivoidaan, paikallisen laitteen estonpoistomekanismeihin.

[71] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 89 kohta.
[72] Yleisen tietosuoja-asetuksen 28 artiklan 3 kohta.
[73] Yleisen tietosuoja-asetuksen 32 artiklan 1 kohdan d alakohta.
[74] Skenaarion 1 suojatoimissa olevat viittaukset biometriseen malliin vastaavat viittauksia avaimeen/salasanaan skenaariossa 2.

C.1.2 Toteutetaan suojatoimia, joilla estetään vääriä positiivia tuloksia, toisena henkilönä esiintymistä ja petoksia.[75]

C.1.3 Kielletään ulkopuolisten pääsy tunnistetietoihin ja biometrisiin tietoihin.[76]

C.1.4 Varmistetaan, että käsittely suoritetaan paikallisesti rekisteröinti-, siirto- ja vertailuvaiheissa. Paikan, jossa vertailu tehdään, olisi oltava mahdollisimman lähellä henkilön laitetta. Sen mahdollistaminen, että mallin vertailu tapahtuu henkilökohtaisessa laitteessa, saattaa edellyttää vuorovaikutusta lentoaseman ulkopuolella sijaitsevien palveluntarjoajien kanssa ja julkisten verkkoresurssien käyttöä, mutta haittapuolena on, että tämä vaikuttaa käytettävyyteen ja levittää mallin ulkopuolisten toimijoiden saataville.

C.1.5 Todennetaan käyttäjän henkilöllisyys uuden lennon lisäämiseksi ja uuden salatun QR-koodin luomiseksi.

C.1.6 Toteutetaan toimenpiteitä sellaisen tilanteen korjaamiseksi, jossa matkustaja voi menettää mahdollisuuden käyttää QR-koodiaan.

C.2 Infrastruktuuri ja verkko

C.2.1 Käyttöjärjestelmää koskevat ehdot pidetään ajan tasalla ja huolehditaan siitä, että laitteen käyttämiseksi edellytettävän todennuksen on oltava käytössä, jotta sovellus / digitaalinen lompakko toimisi. Tähän sisältyy tunnistetietojen ja biometristen tietojen automaattinen poistaminen, jos käyttöjärjestelmä on vanhentunut ja aiheuttaa turvallisuusriskejä.

C.2.2 Eristetään vertailun suorittavat yksiköt (eli tarkastuslaitteet) verkosta niiden ollessa toiminnassa ja toteutetaan kaikki muut tarvittavat toimenpiteet turvallisuuden varmistamiseksi.

C.2.3 Biometrinen vertailu suoritetaan matkustajan laitteella tai tarkastuslaitteella (reunalaskenta).

C.2.4 Tarjotaan ratkaisuja matkustajien henkilökohtaisten laitteiden turvallisuuspuutteiden korjaamiseksi, muun muassa (vähintään) biometristen tietojen ja tunnistetietojen salaus laitteen ollessa lepotilassa.

[75] ENISAn raportti *Digital Identity on leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust*, tammikuu 2022.
[76] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 89 kohta.

C.2.5 Käytetään (vähimmäisvaatimuksena) vain käyttäjän hallussa olevien biometristen tietojen[77] turvallista tallennusta esimerkiksi älypuhelimessa olevan suojatun alijärjestelmän avulla.

C.2.6 Toteutetaan suojatoimia, joilla varmistetaan tilojen, myös lentoaseman biometrisen päätelaitteen, fyysinen turvallisuus. Varmistetaan tunnistetietoja ja biometrisiä tietoja käsittelevien rakenneosien (esimerkiksi laskenta, tietovirta, tilapäinen tai pitkäaikainen tallennus) korkea turvallisuustaso.

C.3 Käyttäjän henkilöllisyyden tarkistamiseen liittyvä tietoturva ja tiedonhallinta

C.3.1 Jaetaan tiedot siirtämisen ja säilytyksen aikana vähintään kolmeen erilliseen ryhmään, kuten tunnistetietoihin, biometrisiin tietoihin ja lentotietoihin.[78] Varmistetaan, että tiedot salataan asianmukaisesti siirtämisen ja säilytyksen välillä.

C.3.2 Otetaan käyttöön teknisiä toimenpiteitä sen varmistamiseksi, että tarkastuspisteessä käsitellään ja todennetaan ainoastaan tietoja, joita voidaan käsitellä laillisesti tietyissä tarkastuspisteissä.

C.3.3 Varmistetaan tietojen tehokas poistaminen[79] suojatulla poistamismenettelyllä (esimerkiksi keskusmuisti, välimuisti ja mahdolliset varmuuskopiot) ja arvioidaan, olisiko tietojen poistaminen automatisoitava. Tietojen säilytysaikojen noudattamista olisi valvottava tiukasti automaattisten rutiinien avulla ilman, että henkilön tarvitsee toteuttaa lisätoimia.[80]

C.3.4 Varmistetaan tietojen (esimerkiksi allekirjoituksen) aitous ja eheys.[81]

C.3.5 Säilytetään matkustajien biometriset tiedot rekisteröintipisteessä ja tarkastuspisteessä vain hyvin lyhyen ajan ja poistetaan ne heti, kun matkustaja on kulkenut tarkastuspisteen läpi.

C.3.6 Jos rekisteröintiin käytetään jotain sovellusta, sovelletaan mobiilisovellusten turvallisuutta koskevia turvallisuusstandardeja sekä kolmannen osapuolen suorittamia turvallisuustestejä sovellusta kehitettäessä.

C.3.7 Varmistetaan, että lentoasemalla on rekisteröintivaiheessa käytössä turvatoimenpiteitä matkustajan biometristen tietojen luottamuksellisuuden ja eheyden säilyttämiseksi. Jos esimerkiksi QR-koodi tulostetaan automaatilla, QR-koodia ei saisi näyttää automaatin näytöllä, jotta pahantahtoinen toimija ei voi ottaa siitä kuvaa. Lyhyen kantaman siirroissa

[77] Skenaarion 1 suojatoimissa olevat viittaukset biometriseen malliin vastaavat viittauksia avaimeen/salasanaan skenaariossa 2.
[78] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 89 kohta.
[79] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 89 kohta.
[80] Tietosuojaneuvoston ohjeet 4/2019 25 artiklassa vahvistetusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 82 kohta.
[81] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 89 kohta.

siirtäminen olisi suoritettava käyttäjän aktiivisen osallistumisen perusteella ja läheisyyden varmistavan kanavan kautta.

C.3.8 Tiedot, jotka ovat yksinomaan henkilön hallussa[82], olisi säilytettävä turvallisesti henkilön laitteella, ja laitteen käyttöjärjestelmiin liittyvät mahdolliset haavoittuvuudet olisi korjattava asianmukaisilla tietoturvakorjauksilla. Jos kyseessä on tulostettu QR-koodi, henkilölle on ilmoitettava sen sisältämien tietojen erityisestä arkaluonteisuudesta ja siitä, mitä sen nojalla voidaan suorittaa.

C.3.9 Varmistetaan, että rekisteröinti suoritetaan asianmukaisia henkilöllisyyden etätodentamistekniikoita noudattaen.[83]

3.2.2 Skenaario 2: rekisteröidyn biometrisen mallin keskitetty tallennus salatussa muodossa lentoasemalla ja yksinomaan matkustajien hallussa olevalla avaimella/salasanalla suojattuna todentamista varten

48. Tässä jaksossa tarkastellaan, onko matkustajien rekisteröityjen biometristen mallien keskitetty säilyttäminen keskitetyssä tietokannassa salatussa muodossa ja yksinomaan matkustajan hallussa olevalla avaimella/salasanalla suojattuna todentamista varten[84], jäljempänä '**skenaario 2**' yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa. Tässä jaksossa tarkastellaan myös skenaariota 2 koskevia asianmukaisia suojatoimia yleisen tietosuoja-asetuksen 25 ja 32 artiklan valossa.

Skenaarion kuvaus

49. Skenaariossa 2 rekisteröinti tehdään vain kerran, ja se on voimassa tietyn ajan (esimerkiksi yhden vuoden ajan viimeisen lennon jälkeen passin voimassaolon päättymiseen asti). Se tehdään joko etänä asianmukaisella tunnistamisen varmuustasolla (esimerkiksi eIDAS-kehyksen asianmukaisella varmuustasolla) tai lentoaseman päätelaitteilla. Rekisteröintiä valvoo lentoaseman pitäjä, ja se koostuu avaimella/salasanalla salattujen tunnistetietojen ja biometristen tietojen tuottamisesta.

50. Tietokanta säilytetään lentoaseman tiloissa lentoaseman pitäjän valvonnassa. Kunkin henkilön henkilökohtaisia avaimia/salasanoja säilytetään vain henkilön laitteella (esimerkiksi lentoaseman pitäjän mobiilisovelluksessa). Sovellus voi luoda avaimen/salasanan sisältävän QR-koodin, joka voidaan joko tulostaa paperille tai näyttää laitteen näytöllä.[85] Lisäksi lentoaseman pitäjä toteuttaa toisen salauskerroksen[86], jonka avaimet ovat lentoaseman pitäjän hallussa.

51. Matkustajien henkilöllisyys todennetaan (yksi yhteen -vertailu), kun he kulkevat lentoaseman tiettyjen tarkastuspisteiden läpi. Biometristen tarkastuspisteiden läpi kulkevat matkustajat esittävät QR-

[82] Skenaarion 1 suojatoimissa olevat viittaukset biometriseen malliin vastaavat viittauksia avaimeen/salasanaan skenaariossa 2.
[83] Ks. ENISAn raportti *Remote ID Proofing: Analysis of methods to carry out identity proofing remotely*, maaliskuu 2021.
[84] Pyynnön liitteessä I olevan käyttötapauksen 2 mukaisesti.
[85] Ranskan valvontaviranomainen on selventänyt, että vaadittujen tietojen lähettämiseen voi olla olemassa myös muita teknisiä ratkaisuja, kuten lyhyen kantaman viestintäprotokolla.
[86] Avain/salasana (joka on henkilön hallussa) salataan toisella avaimella, joka on lentoaseman pitäjän hallussa.

koodinsa erityiselle tarkastuslaitteelle, jossa on QR-koodinlukija ja kamera. Matkustajan indeksoidut tiedot lähetetään tietokantaan ja niiden avulla pyydetään salattu malli, joka ladataan ja tarkastetaan paikallisesti tarkastuslaitteella ja/tai käyttäjän laitteella. Tarkastuspisteen virkailija saa tietoonsa vain vertailun tuottaman osuman ja voi käyttää vain sitä.[87]

52. Tässä skenaariossa tunnistetietoja ja biometrisiä tietoja ei siirretä lentoasemien välillä eivätkä keskitetyt tietokannat ole keskenään yhteenliitettäviä eivätkä yhteentoimivia.

Tietosuojaneuvoston arvio

53. Skenaariossa 2 matkustajien rekisteröidyt biometriset mallit säilytetään keskitetysti, mutta salatussa muodossa ja yksinomaan matkustajien hallussa olevalla avaimella/salasanalla suojattuina. Skenaariossa 2 matkustajien henkilöllisyys todennetaan (yksi yhteen -vertailu).

54. Tässä skenaariossa tavoite matkustajavirran sujuvoittamisesta (nopeuttamalla tarkastuksia) voitaisiin saavuttaa keskitetyn järjestelmän avulla. Tietosuojaneuvosto on aiemmin todennut, että tällaista ratkaisua voitaisiin pitää toteuttamiskelpoisena vaihtoehtona rekisteröityjen biometristen mallien hajautetulle säilytykselle[88] (kuten skenaariossa 1), jos se on objektiivisten tarpeiden mukaista ja asianmukaiset suojatoimet toteutetaan (ks. jäljempänä 60 kohdassa kuvatut suojatoimet).

55. Turvallisuusnäkökohtien osalta kunkin henkilön tiedot salataan erityisellä avaimella, joka on vain kyseisen henkilön hallussa ja hänen yksinomaisessa valvonnassaan. Myös se, että vertailun edellyttämien tietojen (esimerkiksi salasanan/avaimen) on oltava henkilön antamia, toimii toisena todentamisen turvallisuutta vahvistavana tekijänä.[89] Lisäksi lentoaseman pitäjä toteuttaa toisen salauskerroksen, jonka avaimet ovat lentoaseman pitäjän hallussa. Skenaariossa 2 henkilön indeksoidut tiedot lähetetään keskustietokantaan yksilöön liittyvien biometristen tietojen hakemiseksi. Tämän jälkeen tiedot lähetetään (salattuina) tarkastuspisteessä olevaan tietokoneeseen, jossa salaus puretaan, jotta vertailu voidaan suorittaa. Tarkastuspisteen virkailija saa tietoonsa vain osuman ja voi käyttää vain sitä. Jos henkilön avain/salasana säilytetään tarkastuspisteessä olevassa tietokoneessa ja keskustietokantaan lähetetään ainoastaan matkustajan indeksoidut tiedot salatun biometrisen mallin saamiseksi, tällaisten turvallisuustoimien voidaan katsoa olevan yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan mukaisia.

56. Yleisen tietosuoja-asetuksen 25 artiklan mukaisuuden osalta ja erityisesti tietojen minimointia koskevan vaatimuksen noudattamiseksi olisi varmistettava, että käsittely on tarpeellisuuden periaatteen mukaista. Skenaariossa 2 valittujen toimenpiteiden voidaan katsoa täyttäneen tarpeellisuuden periaatteen tavoiteltuun tarkoitukseen (eli lentoasemien matkustajavirtojen sujuvoittamiseen) nähden, jos rekisterinpitäjä voi käsittelyn olosuhteista riippuen osoittaa, ettei ole olemassa yksityisyyteen vähemmän puuttuvia vaihtoehtoisia ratkaisuja, joilla sama tavoite voitaisiin saavuttaa yhtä tehokkaasti. Skenaariossa 2 matkustajien olisi silti esitettävä laitteensa.[90] Tästä

[87] Ranskan valvontaviranomainen selvensi, että tämä säilytysaika on vain havainnollistava ja sitä voidaan pitää hyväksyttävänä, koska avain on henkilöiden hallussa ja se voidaan valita rekisteröintivaiheessa. On kuitenkin huomattava, että tällaista säilytysaikaa voidaan mukauttaa.

[88] Videolaitteita koskevat tietosuojaneuvoston ohjeet 3/2019, 88 kohta.

[89] Tämä vähentää esimerkiksi toisena henkilönä esiintymisen riskiä. Ks. myös suojatoimi C.1.2.

[90] Ranskan valvontaviranomainen on selventänyt, että mallin esittämiseksi saattaa olla myös muita vaihtoehtoja, kuten paperituloste. Lisäksi tietosuojaneuvosto on tietoinen siitä, että tulevaisuudessa voitaisiin käyttää esimerkiksi lähitiedonsiirtojärjestelmään perustuvaa vaihtoehtoista teknologiaa.

huolimatta rekisterinpitäjä saattaa pystyä osoittamaan, että skenaario 2 nopeuttaa todentamisprosessia nykytilanteeseen verrattuna, jossa ihminen tarkastaa, vastaako tarkastuskortissa oleva nimi matkustajan henkilöllisyystodistusta[91], tai skenaarioon 1 verrattuna. Tätä ei voitaisi osoittaa, jos matkustajien henkilöllisyyttä ei tällä hetkellä tarkasteta virallisen henkilöllisyystodistuksen perusteella (ks. edellä 18 kohta).

57. Oikeasuhteisuuden periaatteen osalta tällaisesta käsittelystä johtuvaa yksityisyyteen puuttumista voidaan tasapainottaa matkustajien aktiivisella osallistumisella, koska heidän salatut tietonsa ovat yksinomaan heidän valvonnassaan. Lisäksi vaikuttaa siltä, että matkustajien biometristen tietojen tallentamisesta keskitettyyn tietokantaan ja yksinomaan matkustajien hallussa olevasta avaimesta aiheutuvia turvallisuusriskejä voidaan lieventää asianmukaisilla suojatoimilla (ks. jäljempänä 60 kohdassa käsitellyt suojatoimet). Mikäli rekisterinpitäjä toteuttaa kyseisen käsittelyn edellyttämät asianmukaiset suojatoimet, henkilöihin kohdistuvia riskejä voitaisiin lieventää ja rekisteröityjen perusoikeuksiin ja -vapauksiin kohdistuvaa kielteistä vaikutusta voitaisiin pitää oikeasuhteisena ennakoituun hyötyyn nähden. Kussakin tapauksessa olisi tietenkin varmistettava, että vain kyseiseen tarkoitukseen tarvittavia tietoja käsitellään ja että vain suostumuksen antaneet matkustajat tarkastetaan, jolloin ei ole vaaraa siitä, että biometrisiä tietoja kerättäisiin muilta matkustajilta, jotka eivät ole antaneet suostumustaan.

58. Pyynnössä todetaan esimerkkinä, että skenaariossa 2 salattujen tietojen säilytysaika tietokannassa voisi tavallisesti olla yksi vuosi henkilön viimeisen lennon jälkeen ja passin voimassaolon päättymiseen asti. Pyynnössä ei esitetä mitään objektiivisia syitä näin pitkän ajanjakson perustelemiseksi, mutta voidaan olettaa, että tällaisella säilytysajalla on tarkoitus sujuvoittaa tulevia lentoja. Jotta tämä skenaario olisi säilytysajan osalta yhteensopiva yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan kanssa, rekisterinpitäjien olisi pystyttävä perustelemaan, miksi valittu säilytysaika on tarpeen kussakin tapauksessa kyseessä olevaa tarkoitusta varten. Tietosuojaneuvosto suosittelee, että rekisterinpitäjät suunnittelevat mahdollisimman lyhyitä säilytysaikoja ottaen huomioon myös hyvin harvoin lentävät matkustajat ja tarjoavat matkustajille mahdollisuuden valita haluamansa säilytysajan.

59. Edellä esitetyn perusteella tietosuojaneuvosto katsoo kysymyksen 2.1.1 osalta, että tällaisen käsittelyn **voitaisiin periaatteessa katsoa olevan yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan, 25 artiklan ja 32 artiklan kanssa, mikäli toteutetaan asianmukaiset suojatoimet**.

Asianmukaiset suojatoimet

60. Tällaisessa skenaariossa tietosuojaneuvosto katsoo kysymyksen 2.1.2 osalta, että **skenaariossa 1 lueteltujen suojatoimien lisäksi** olisi toteutettava ainakin seuraavat suojatoimet. Muita kuin tässä lausunnossa kuvattuja suojatoimia voitaisiin käyttää samojen turvallisuus- ja tietosuojatavoitteiden saavuttamiseksi, ja ne voivat olla laillisia, mikäli niillä varmistetaan sovellettavien oikeudellisten kehysten noudattaminen.

61. Huomautus: *Tämä on yleistasoinen ja viitteellinen yleiskatsaus mahdollisista asianmukaisista suojatoimista, jotka rekisterinpitäjä voisi toteuttaa skenaarion 2 kaltaisessa ratkaisussa. Niiden*

[91] Voidaan myös väittää, että biometrinen tarkastus saattaa olla vähemmän virhealtis kuin ihmisen suorittama tarkastus.

asianmukaisuutta yleisen tietosuoja-asetuksen 25 ja 32 artiklan nojalla on analysoitava tapauskohtaisesti. Kaikkien rekisterinpitäjien on varmistettava, että ne suorittavat oman tietosuojaa koskevan vaikutustenarvioinnin, ja niiden kulloisetkin ratkaisut saattavat edellyttää lisätoimenpiteitä, joita ei käsitellä tässä lausunnossa.

D. Yleistä

D.1 Rekisteröityjen oikeudet ja suojatoimet, jotka rekisterinpitäjät voivat toteuttaa

D.1.1 Varmistetaan, että matkustajat voivat valvoa kaikkien tietojensa säilytysaikoja. Säilytysajat olisi rajoitettava siihen, mikä on tarpeen kyseistä tarkoitusta varten. Enimmäissäilytysaika olisi vahvistettava erilaisten tekijöiden, esimerkiksi henkilöasiakirjan voimassaoloajan, perusteellisen analyysin perusteella. Rekisteröidyille olisi tarjottava mahdollisuus valita haluamansa säilytysaika, joka voi olla lyhyempi kuin oletusarvoinen säilytysaika.

D.1.2 Rekisteröidyllä on mahdollisuus milloin tahansa pyytää yksinomaan hänen hallussaan olevien (avain/salasana) ja mobiilisovelluksessa tai digitaalisessa lompakossa säilytettävien tietojen poistamista.[92]

D.1.3 Varmistetaan, että keskustietokanta sijaitsee paikassa, jossa toimivaltainen valvontaviranomainen voi valvoa sitä tehokkaasti.

E. Organisaatio:

E.1 Periaatteet ja säännösten noudattaminen

E.1.1 Keskuspalvelimeen saa luottaa vain rajallisesti. Varmistetaan, että keskuspalvelimen hallinnoinnissa noudatetaan selkeästi määritettyjä sääntöjä ja sen yhteydessä toteutetaan kaikki tarvittavat toimenpiteet keskuspalvelimen turvallisuuden varmistamiseksi.[93]

F. Tekninen ulottuvuus:

F.1 Pääsy tietoihin

F.1.1 Säilytetään lokitiedot siitä, kenellä on pääsy henkilötietoihin, erityisesti tunnistetietoihin ja biometrisiin tietoihin, ja siitä, milloin niitä on käytetty.

F.2 Infrastruktuuri ja verkko

[92] On huomattava, että tämä suojakeino koskee vain skenaariota 2.
[93] Tietosuojaneuvoston ohjeet 4/2020 sijaintitiedoista ja kontaktien jäljitysvälineistä, PRIV-5, s. 17.

F.2.1 Suojataan keskustietokanta asianmukaisesti myös käytettävyyteen kohdistuvilta hyökkäyksiltä.

F.2.2 Varmistetaan, ettei keskustietokantaan, rekisteröintilaitteisiin ja vertailuyksiköihin ole internetyhteyttä. Näiden järjestelmien käyttö ja ylläpito (kuten varmuuskopiointi, korjauspäivitykset ja valvonta) on suoritettava paikallisesti lentoaseman tiloissa.

F.3 Tietoturva ja tiedonhallinta

F.3.1 Käytetään uusimpia salaustekniikoita sovelluksen ja keskuspalvelimen välisen tiedonvaihdon turvaamiseksi.[94]

F.3.2 Säilytetään yksittäinen avain/salasana tasolla, jolla sitä käytetään salauksen purkamiseen (esimerkiksi tarkastuslaitteessa), ja käytetään indeksoituja tietoja vain niitä vastaavan rekisteröidyn biometrisen mallin hakemiseen keskustietokannasta.

F.3.3 Varmistetaan, että kun avain/salasana vaihdetaan käyttäjän laitteen ja tarkastuslaitteen välillä, viestintä on suojattu mahdolliselta salakuuntelulta tai sen välittämiseltä kolmansille osapuolille.

F.3.4 Indeksoidaan biometrinen malli, kun se on tallennettu tietokantaan, jotta voidaan varmistaa yksi yhteen -todennus ja varmistaa, että malli on yksilöllinen ja liittyy henkilöön. Varmistetaan, ettei indeksoitu malli paljasta mitään matkustajan tunnistetietoja eikä ole yhteydessä salausavaimeen.

F.3.5 Todennetaan ja salataan riittävästi keskustietokannan ja tarkastuspisteiden väliset siirrot ja sijoitetaan ne erillisiin verkkoihin.

F.3.6 Vältetään kaksisuuntaisia linkkejä tietokokonaisuuksien (tunnistetiedot ja biometriset tiedot sekä lentotiedot) välillä ja säilytetään tietokannassa vain asiaankuuluvat yksisuuntaiset linkit, esimerkiksi vain yksisuuntaiset linkit indeksoidusta mallista tunnistetietoihin, indeksoidusta mallista salattuihin biometrisiin tietoihin ja indeksoidusta mallista lentotietoihin.

F.3.7 Varmistetaan toiminnan jatkuvuutta koskevat järjestelyt, kuten asianmukaiset varasäilytysjärjestelmät.

F.3.8 Varmistetaan, että tarkastuslaite ei säilytä lokitietoja salatuista tai salaamattomista malleista.

[94] Tietosuojaneuvoston ohjeet 4/2020 sijaintitiedoista ja kontaktien jäljitysvälineistä, PRIV-4, s. 16: ”Tällaisia tekniikoita ovat esimerkiksi seuraavat: symmetrinen ja epäsymmetrinen salaus, tiivistysfunktiot, Private Membership Test (PMT) -protokollat, Private Set Interaction (PSI) -protokollat, Bloom-suodattimet, Private Information Retrieval (PRI) -protokolla, homomorfinen salaus jne.”

3.2.3 Rekisteröityjen biometristen mallien keskitetty säilyttäminen tunnistamista varten

62. Tässä jaksossa tarkastellaan, onko matkustajien rekisteröityjen biometristen mallien keskitetty säilyttäminen tunnistamista varten yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan kanssa, jos malleja ei ole salattu yksinomaan matkustajan hallussa olevalla avaimella/salasanalla, kahdessa käyttötapauksessa: 1) kun tällaiset mallit säilytetään lentoasemalla sijaitsevassa ja lentoaseman pitäjän valvonnassa olevassa tietokannassa[95], jäljempänä '**skenaario 3.1**', ja 2) kun tällaiset mallit tallennetaan lentoyhtiön valvonnassa olevaan pilvipalveluun[96], jäljempänä '**skenaario 3.2**'.

63. Tietosuojaneuvosto katsoo, että biometristen tietojen käyttö **tunnistustarkoituksiin** suurissa keskustietokannoissa puuttuu rekisteröityjen perusoikeuksiin ja saattaa aiheuttaa vakavia seurauksia rekisteröidyille.[97] Lisäksi biometristen tietojen käyttöä olisi tarkasteltava tarpeellisuuden ja oikeasuhteisuuden periaatteiden valossa suhteessa siihen tarkoitukseen, jota varten niitä käsitellään.[98]

3.2.3.1 Skenaario 3.1: keskitetty säilyttäminen lentoasemalla sijaitsevassa ja lentoaseman pitäjän valvonnassa olevassa tietokannassa

Skenaarion kuvaus

64. Skenaariossa 3.1 matkustajan rekisteröity biometrinen malli tallennetaan lentoaseman tiloissa sijaitsevaan ja lentoaseman pitäjän valvonnassa olevaan keskustietokantaan salatussa muodossa. Matkustajien tiedot lokeroidaan, mikä tarkoittaa, että heidän henkilötietonsa, rekisteröity biometrinen mallinsa ja lentotietonsa tallennetaan kolmeen erilliseen tietokantaan. Tällaiset tiedot salataan eri avaimilla sekä säilytyksen aikana että siirrettäessä niitä palvelimille, joilla vertailu suoritetaan, jolloin lentoaseman pitäjä purkaa niiden salauksen.

65. Matkustajien on rekisteröidyttävä jokaista lentoa varten melko vähän aikaa (esimerkiksi 48 tuntia) ennen lennon lähtöä. Tällainen rekisteröinti voidaan suorittaa joko etänä tai lentoaseman päätelaitteilla asianmukaisella tunnistamisen varmuustasolla (esimerkiksi eIDAS-kehyksen asianmukaisella varmuustasolla). Vaihtoehtoisesti rekisteröinti voidaan toteuttaa skenaariossa 1 kuvatulla tavalla, jolloin matkustajien on siirrettävä tietonsa digitaalisista lompakoistaan lentoaseman järjestelmään lähtöään edeltävien 48 tunnin kuluessa.

66. Myös tässä skenaariossa matkustajat esittäytyvät kameralla varustetulle tarkastuslaitteelle. Tämän jälkeen heidän biometrinen näytteensä lähetetään lentoaseman keskuspalvelimelle, joka vertailee tietoja keskitetyn biometrisen tietokannan tietoihin. Tällä tavoin matkustaja on mahdollista tunnistaa ja voidaan tarkastaa, onko hän todella rekisteröitynyt lähtevälle lennolle (tai siirtymään koneeseen, jos tarkastus suoritetaan koneeseen siirryttäessä). Tarkastuspisteestä riippuen käsittelypyynnön

[95] Pyynnön liitteessä I olevan käyttötapauksen 3A mukaisesti.
[96] Pyynnön liitteessä I olevan käyttötapauksen 3B mukaisesti.
[97] Ks. esimerkiksi biometrisiä tekniikkoja koskeva tietosuojatyöryhmän lausunto 3/2012, s. 8. Ks. myös edellä 26 kohta.
[98] Yleisen tietosuoja-asetuksen johdanto-osan 4 kappale. Ks. myös biometrisiä tekniikkoja koskeva tietosuojatyöryhmän lausunto 3/2012, s. 8.

esittäneelle tarkastuspisteen virkailijalle takaisin lähetettävät tiedot voidaan minimoida, ja ne voivat olla esimerkiksi kyllä-/ei-vastaus tai tarvittaessa itse vertailun tuottama osuma. Tässä tapauksessa tarkastuspisteen valvojalle lähetetään vain käsittelypyynnön tulos ja hän käyttää vain sitä.

67. Tässä skenaariossa matkustajat tunnistetaan (1:N- eli yksi moneen -vertailu, jossa N on lentoasemalla useiden päivien aikana odotettavissa oleva matkustajamäärä). Lisäksi biometrinen vertailu suoritetaan vasta kunkin matkustajan saapuessa lähtölentoaseman ennalta määriteltyihin tarkastuspisteisiin, mutta itse tietojenkäsittely tapahtuu keskustietokantaan liitetyssä keskuspalvelimessa. Tässä skenaariossa säilytysaika on tavallisesti 48 tuntia, ja tiedot poistetaan lentokoneen lähdettyä.

Tietosuojaneuvoston arvio

68. Kuten edellä on todettu, biometristen tietojen käsittely lisää rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä.[99] Näin ollen tietoturvan puutteilla voi olla rekisteröityjen kannalta erityisen vakavia seurauksia.[100] Rekisterinpitäjien velvollisuutena on vähentää näitä riskejä tehokkaasti. Koska tässä skenaariossa koko rakenne on täysin keskitetty, matkustajat menettävät suuremmassa määrin mahdollisuuden valvoa tietojaan. Lisäksi myös riski siitä, että tietoja käsitellään muihin tarkoituksiin kuin matkustajavirtojen hallintaan, saattaa kasvaa.

69. Turvallisuutta koskevan periaatteen ja siihen liittyvien vaatimusten (yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohta ja 32 artikla) valossa olisi katsottava, että tunnistetietojen ja biometristen tietojen säilyttäminen keskitetysti, vaikkakin erillisissä tietokannoissa, voi tarjota merkittäviä hyökkäyspisteitä, ja tällaisen tietokannan luottamuksellisuuden rikkominen voi myöhemmässä vaiheessa johtaa siihen, että hyökkääjä saa pääsyn koko tietokokonaisuuteen. Näin ollen mahdollinen kasvontunnistusmalleihin ja niihin liittyviin tunnistetietoihin kohdistuva tietoturvaloukkaus saattaa mahdollistaa rekisteröityjen luvattoman tai laittoman tunnistamisen muissa ympäristöissä. Se saattaa myös vaarantaa kasvojentunnistusmallien myöhemmän turvallisen käytön tunnisteena sen mukaan, mitä menetelmiä biometriseen tunnistamiseen on käytetty. Siinä tapauksessa tietoturvaloukkauksen vaikutuksia ei voida lieventää, toisin kuin silloin, jos käytetään muun tyyppisiä tunnuksia (kuten käyttäjätunnusta tai salasanaa), joita voidaan muuttaa.[101]

70. Lisäksi rekisterinpitäjän hallussa olevien tunnistetietojen ja biometristen tietojen suuri määrä ja laatu tekevät niistä hyökkääjälle erittäin arvokkaan kohteen, mikä lisää turvallisuusriskin todennäköisyyttä. Lisäksi tietoturvaloukkauksilla voisi olla suurempi vaikutus, koska tietojen keskitetyn säilytyksen vuoksi hyökkääjien voisi olla helpompi saada käyttöönsä useita matkustajia koskevia henkilötietoja. Tästä syystä mahdollinen tietoturvaloukkaus voisi altistaa suuren määrän rekisteröityjä laajamittaisen identiteettivarkauden kaltaisille vakaville riskeille, joita on äärimmäisen vaikea lieventää.

71. Näin ollen yhteensopivuudesta yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan kanssa on todettava, että kun otetaan huomioon uusin tekniikka, skenaariossa 3.1

[99] Ks. edellä oleva 26 kohta.

[100] Yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn Euroopan neuvoston yleissopimuksen neuvoa-antavan komitean antamat kasvojentunnistusta koskevat suuntaviivat, kesäkuu 2021, s. 22.

[101] Ks. tähän liittyen biometrisiä tekniikkoja koskeva tietosuojatyöryhmän lausunto 3/2012, s. 34.

suunnitellut toimenpiteet[102] eivät riitä varmistamaan riskiä vastaavaa turvallisuustasoa. Tällä perusteella skenaarion 3.1 mukainen käsittely ei olisi yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan kanssa, jos rekisterinpitäjä toteuttaa vain nämä toimenpiteet.

72. Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdassa säädetyn periaatteen mukaisesti biometristen tietojen säilytysaika keskustietokannassa on tässä skenaariossa tavallisesti 48 tuntia. Tällainen säilytyksen rajoittaminen vaikuttaisi vähentävän merkittävästi henkilötietoihin kohdistuviin tietoturvaloukkauksiin liittyviä riskejä. Tietojen säilytysaika ei kuitenkaan yksinään ole ratkaiseva tekijä kyseisen rakenteen yleisen yhteensopivuuden kannalta, koska rekisterinpitäjät voivat muuttaa säilytysaikoja. Ehdotettujen toimenpiteiden on joka tapauksessa täytettävä yleisen tietosuoja-asetuksen 25 artiklan mukaiset sisäänrakennettua ja oletusarvoista tietosuojaa koskevat vaatimukset.

73. Toisin kuin skenaarioissa 1 ja 2, joissa matkustajien henkilöllisyys todennetaan, skenaariossa 3.1 matkustajat tunnistetaan (1:N- eli yksi moneen -vertailu, jossa N on sellaisten lentoasemalla useiden päivien aikana odotettavissa olevien matkustajien määrä, jotka ovat antaneet suostumuksensa tällaiseen käsittelyyn heidän kulkiessaan lentoasemalla tiettyjen tarkastuspisteiden läpi). Tämä edellyttää matkustajien hakua keskustietokannasta käsittelemällä jokaista otettua biometristä näytettä sen tarkistamiseksi, vastaako se jotakuta järjestelmän tuntemaa henkilöä. Toisin kuin skenaariossa 2, skenaariossa 3.1 avaimet eivät ole pelkästään matkustajien hallussa. Näin ollen matkustajilla on tässä skenaariossa huomattavasti pienempi mahdollisuus valvoa biometrisiä tietojaan. Sen vuoksi skenaariossa 3.1 ehdotettu käsittely ei voi olla yhteensopivaa yleisen tietosuoja-asetuksen 25 artiklan mukaisten sisäänrakennettua ja oletusarvoista tietosuojaa koskevien vaatimusten kanssa.

74. Yleisen tietosuoja-asetuksen 25 artiklan perusteella rekisterinpitäjien olisi otettava huomioon käsittelyssä tarvittavien henkilötietojen tyypit, ryhmät ja yksityiskohtaisuus.[103] Näissä suunnitteluvalinnoissa olisi otettava huomioon, että tietojen minimoinnin, eheyden ja luottamuksellisuuden sekä säilytyksen rajoittamisen periaatteisiin kohdistuvat riskit kasvavat, kun kerätään suuria määriä yksityiskohtaisia henkilötietoja, kun taas riskit pienenevät, kun rekisteröidyistä kerätään pienempiä määriä ja/tai vähemmän yksityiskohtaisia tietoja. Joka tapauksessa oletusasetuksena ei saa olla, että kerätään sellaisia henkilötietoja, jotka eivät ole tarpeen tietyn käsittelytarkoituksen kannalta. Toisin sanoen jos tietyt henkilötietoryhmät ovat tarpeettomia tai jos yksityiskohtaisia tietoja ei tarvita, koska vähemmän yksityiskohtaisetkin tiedot riittävät, henkilötietoja ei saa kerätä yhtään enempää kuin on tarpeen. Jos tässä tapauksessa jollain toisella käsittelyn toteutustavalla voitaisiin saavuttaa sama tavoite ja se on käytettävissä skenaariossa 3.1 kuvattujen ehtojen mukaisesti, kasvontunnistusteknologiaa ei ole tarpeen käyttää.

75. Yleisen tietosuoja-asetuksen 25 artiklan osalta keskeinen sisäänrakennettua ja oletusarvoista tietosuojaa koskeva seikka on rekisteröidyn itsemääräämisoikeus. Rekisteröidylle on etenkin taattava mahdollisimman suuri itsemääräämisoikeus omien henkilötietojensa käytön määrittämisessä sekä

[102] Jotka on kuvattu edellä 64–67 kohdassa.

[103] Tietosuojaneuvoston ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 49 kohta.

kyseisen käytön että käsittelyn laajuuden ja ehtojen osalta.[104] Skenaariossa 1 rekisteröidyllä olisi itsemääräämisoikeus ja valvontamahdollisuus biometristen malliensa käytön, luovuttamisen ja poistamisen suhteen, ja skenaariossa 2 rekisteröity säilyttäisi jonkin verran määräysvaltaa oman biometrisen mallinsa luovuttamiseen, koska salausavain/salasana säilytettäisiin heidän hallussaan. Skenaariossa 3.1 rekisteröity on kuitenkin täysin riippuvainen biometristen tietojensa käsittelyä koskevista rekisterinpitäjän valinnoista eikä siten voi suoraan valvoa biometrisen mallinsa käyttöä.

76. Yleisen tietosuoja-asetuksen 25 artiklan mukaisuuden ja erityisesti tietojen minimointia koskevan vaatimuksen noudattamisen osalta skenaarion 3.1 mukainen käsittely ei olisi tarpeellisuuden periaatteen mukaista. Tietosuojaneuvosto katsoo, että samankaltainen tulos lentoasemien matkustajavirtojen sujuvoittamiseksi voidaan saavuttaa yksityisyyteen vähemmän puuttuvalla tavalla. Se voidaan saavuttaa esimerkiksi käyttämättä biometrisiä tietoja (joskin käyttäjäkokemus olisi tällöin erilainen, koska tarkistuskortin ja tarvittaessa virallisen henkilöllisyystodistuksen esittäminen voi kestää kauemmin). Lisäksi muut ratkaisut, erityisesti ne, jotka perustuvat biometristen tietojen säilyttämiseen henkilön laitteella olevassa paikallisessa lompakossa tai edellyttävät tietojen salaamista tietyllä henkilön laitteelle tallennetulla avaimella, mahdollistavat tavoitteiden saavuttamisen yksityisyyteen vähemmän puuttuvalla tavalla.

77. Oikeasuhteisuuden periaatteen osalta skenaarion 3.1 mukainen käsittely aiheuttaisi rekisteröityjen oikeuksiin kohdistuvia riskejä, joita suunnitellut toimenpiteet eivät lieventäisi, kun otetaan huomioon uusin tekniikka. Hyvin monien henkilöiden biometrisia tietoja sisältävään keskitettyyn tietokantaan kohdistuvan tietoturvaloukkauksen mahdollisesti aiheuttama riski rekisteröityjen perusoikeuksiin ja -vapauksiin kohdistuvasta kielteisestä vaikutuksesta näyttää olevan suurempi kuin käsittelystä odotettavissa oleva hyöty, koska tällainen hyöty, eli tarkastusten lievä helpottuminen ja nopeutuminen, on suhteellisen vähäinen. Sen vuoksi tämä hyöty ei voi oikeuttaa tällaisia yksilöiden perusoikeuksiin ja -vapauksiin voimakkaasti puuttuvia toimenpiteitä eikä skenaarion 3.1 mukainen käsittely ole oikeasuhteisuuden periaatteen mukainen.

78. Näiden seikkojen perusteella tietosuojaneuvosto toteaa kysymyksen 2.2.1 osalta, että kun käsittely suoritetaan nimenomaisesti lentoasemien matkustajavirtojen sujuvoittamiseksi, skenaariossa 3.1 suunniteltu käsittely

    - **ei voi olla yhteensopivaa yleisen tietosuoja-asetuksen 25 artiklan kanssa**
    - **ei olisi yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan kanssa**, jos rekisterinpitäjä toteuttaisi vain skenaariossa 3.1 kuvatut toimenpiteet.

[104] Tietosuojaneuvoston ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta, 70 kohta. Yleisen tietosuoja-asetuksen johdanto-osan 7 kappaleessa selvennetään lisäksi, että ”[l]uonnollisten henkilöiden olisi voitava valvoa omia henkilötietojaan”.

3.2.3.2 Skenaario 3.2: keskitetty säilytys pilvipalvelussa, joka on lentoyhtiön valvonnassa

Skenaarion kuvaus

79. Skenaariossa 3.2 matkustajan rekisteröity biometrinen malli tallennetaan pilvipalveluun, joka on lentoyhtiön tai sen pilvipalveluntarjoajan (tietojen käsittelijän) valvonnassa. Pyynnössä täsmennetään, että pilvipalveluntarjoaja sijaitsisi ETA:n alueella.[105] Tässä tapauksessa matkustajien tiedot salataan, mutta salaus puretaan, kun tietoja käytetään (esimerkiksi kun suoritetaan vertailu) ja avaimet ovat lentoyhtiön tai sen pilvipalveluntarjoajan hallinnassa. Matkustajien biometrisiä tietoja käytetään matkustajien tunnistamiseen (1:N- eli yksi moneen -vertailu, jossa N voi olla enintään lentoyhtiön asiakkaiden kokonaismäärä).[106]

80. Kuten skenaarioissa 1, 2 ja 3.1, myös tässä tapauksessa matkustajien on ensin rekisteröidyttävä. Skenaariossa 3.2 matkustajien rekisteröinti tehdään kuitenkin kerran ja se on voimassa niin kauan kuin asiakkaalla on tili lentoyhtiössä. Rekisteröinti suoritetaan joko etänä asianmukaisella tunnistamisen varmuustasolla (esimerkiksi eIDAS-kehyksen asianmukaisella varmuustasolla) tai lentoaseman päätelaitteilla. Biometrinen vertailu suoritetaan vasta kun matkustajat saapuvat lentoaseman ennalta määriteltyihin tarkastuspisteisiin, mutta itse tietojenkäsittely tapahtuu pilvipalvelussa.

81. Lentoasemalla matkustajat kulkevat kameralla varustettujen tarkastuslaitteiden läpi. Matkustajien biometriset tiedot lähetetään käsittelypyynnöllä lentoyhtiön pilvipalvelimelle, jossa niitä vertaillaan keskustietokantaan. Tällä tavoin matkustaja on mahdollista tunnistaa ja voidaan tarkastaa, onko hän todella rekisteröitynyt lähtevälle lennolle (tai siirtymään koneeseen, jos tarkastus suoritetaan koneeseen siirryttäessä).

82. Osumat voidaan mahdollisesti asettaa useiden lentoaseman pitäjien saataville, jos lentoyhtiöllä on erityinen käyttöpääte tai pääsy lentoaseman yhteiseen tietojärjestelmäinfrastruktuuriin. Tarkastuspisteestä riippuen käsittelypyynnön esittäneelle tarkastuspisteen virkailijalle takaisin lähetettävät tiedot voidaan minimoida, ja ne voivat olla esimerkiksi kyllä-/ei-vastaus tai tarvittaessa itse vertailun tuottama osuma. Tässä tapauksessa tarkastuspisteen virkailija saa tietoonsa vain käsittelypyynnön tuloksen ja voi käyttää vain sitä.

83. Mallin säilytysajan määrittää lentoyhtiö, ja mallia voidaan mahdollisesti säilyttää niin kauan kuin asiakkaalla on tili lentoyhtiössä.

Tietosuojaneuvoston arvio

84. Tietosuojaneuvoston jo skenaarion 3.1 yhteydessä esittämät näkökohdat[107] pätevät myös tähän skenaarioon.

85. Turvallisuutta koskevan periaatteen ja siihen liittyvien vaatimusten (yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohta ja 32 artikla) osalta skenaariossa 3.2 käsittely tapahtuu pilvipalvelussa ja

[105] Ranskan valvontaviranomainen selvensi, että tämä on vain havainnollistava esimerkki ja että voidaan harkita myös ETA:n ulkopuolella sijaitsevia pilvipalvelujen tarjoajia. Lisäksi voitaisiin harkita muita säilytysratkaisuja (esimerkiksi sellaisia, joissa ei käytetä pilvipalvelua).
[106] Ranskan valvontaviranomainen selvensi, että tämä on vain havainnollistava esimerkki ja että on olemassa ratkaisu, jossa biometrisiä tietoja lähetetään joka kerran ennen lentoa.
[107] Edellä 68–77 kohta.

useilla toimijoilla, mahdollisesti myös ETA:n ulkopuolisilla palveluntarjoajilla, voi olla pääsy tällaisiin tietoihin, vaikka tietoja säilytetään ETA:n alueella.[108] Tällaiseen rakenteeseen sisältyy mahdollisia riskejä, jotka liittyvät henkilötietojen siirtämiseen kolmansiin maihin. Lisäksi matkustajien tiedot salataan, mutta salaus puretaan, kun tietoja käytetään (esimerkiksi kun suoritetaan vertailu), ja avaimet ovat lentoyhtiön tai sen pilvipalveluntarjoajan hallinnassa. Tällainen säilytys voi lisätä entisestään turvallisuusuhkien mahdollisuutta.

86. Näin ollen yhteensopivuudesta yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan kanssa on todettava, että uusin tekniikka huomioon ottaen skenaariossa 3.2 suunnitellut toimenpiteet[109] eivät riitä varmistamaan riskiä vastaavaa turvallisuustasoa. Tällä perusteella skenaarion 3.2 mukainen käsittely ei olisi yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan mukaista, jos rekisterinpitäjä toteuttaa vain nämä toimenpiteet.

87. Lisäksi skenaarion 3.2 mukaan[110] tietoja voitaisiin säilyttää merkittävän ajan (eli mahdollisesti niin kauan kuin rekisteröidyllä on tili lentoyhtiössä). Tällainen säilytysaika altistaa tiedot suuremmille niiden luottamuksellisuuteen ja eheyteen kohdistuvien tietoturvaloukkausten riskeille ja näyttäisi ylittävän sen, mikä on käsittelyn kannalta ehdottoman välttämätöntä ja oikeasuhteista. Tietosuojaneuvosto huomauttaa, että tietojen säilytysaika ei yksinään ole ratkaiseva tekijä sen kannalta, onko kyseinen rakenne yleisesti yhteensopiva yleisen tietosuoja-asetuksen kanssa, koska rekisterinpitäjät voivat muuttaa säilytysaikoja. Tietosuojaneuvoston käytettävissä olevien ja skenaarion 3.2 kuvaukseen sisältyvien tietojen perusteella tälle pitkälle säilytysajalle ei kuitenkaan ole riittävää perustetta eikä skenaarioon sisälly ilmeisiä toimenpiteitä henkilöihin kohdistuvien riskien lieventämiseksi. Tämän perusteella ehdotettu säilytysaika ei rajoittuisi siihen, mikä on tarpeellista, kuten yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdassa säädetty säilytyksen rajoittamista koskeva periaate edellyttää.

88. Skenaariossa 3.2 ehdotetut toimenpiteet eivät joka tapauksessa voi täyttää yleisen tietosuoja-asetuksen 25 artiklassa säädettyjä sisäänrakennettua ja oletusarvoista tietosuojaa koskevia vaatimuksia. Skenaariossa 3.2 matkustajien rekisteröidyt biometriset mallit tallennetaan pilvipalveluun, joka on lentoyhtiön tai sen pilvipalveluntarjoajan (tietojen käsittelijän) valvonnassa. Kuten edellä on selostettu, useilla toimijoilla saattaisi mahdollisesti olla pääsy näihin tietoihin. Lisäksi matkustajien biometrisiä tietoja käytetään matkustajien tunnistamiseen (1:N- eli yksi moneen -vertailu, jossa N voi olla enintään lentoyhtiön käyttäjien/asiakkaiden kokonaismäärä). Tällaisessa menetelmässä henkilö löydetään keskustietokannassa olevasta henkilöryhmästä käsittelemällä jokaista otettua kasvokuvaa sen tarkistamiseksi, vastaako se jotakuta järjestelmän tuntemaa henkilöä. Toisin kuin skenaario 3.1, skenaariossa 3.2 vertailu voitaisiin suorittaa paljon laajemmassa mitassa, koska siinä kriteerinä on lentoyhtiön asiakkaiden kokonaismäärä, kun taas skenaario 3.1 sisältää vain useiden päivien aikana odotettavissa olevien matkustajien määrän.

89. Lisäksi yleisen tietosuoja-asetuksen 25 artiklan mukaisuuden ja erityisesti tietojen minimointia koskevan vaatimuksen noudattamisen osalta skenaarion 3.2 mukainen käsittely ei olisi tarpeellisuuden periaatteen mukaista. Tietosuojaneuvosto katsoo, että samankaltainen tulos

[108] Euroopan tietosuojaneuvosto, *2022 Coordinated Enforcement Action on the use of cloud-based services by the public sector*, 17. tammikuuta 2023, s. 19.
[109] Ks. edellä 79–83 kohta.
[110] Ks. edellä 83 kohta.

lentoasemien matkustajavirtojen sujuvoittamiseksi voidaan saavuttaa yksityisyyteen vähemmän puuttuvilla toimenpiteillä, esimerkiksi käyttämättä biometrisiä tietoja, joskin käyttäjäkokemus olisi tällöin erilainen, koska henkilöllisyystodistuksen ja tarkistuskortin esittäminen saattaa kestää kauemmin. Lisäksi muut ratkaisut, erityisesti ne, jotka perustuvat biometristen tietojen säilyttämiseen henkilön laitteella olevassa paikallisessa lompakossa tai edellyttävät tietojen salaamista tietyllä henkilön laitteelle tallennetulla avaimella, antavat rekisterinpitäjälle mahdollisuuden saavuttaa tavoitteet yksityisyyteen vähemmän puuttuvalla tavalla.

90. Oikeasuhteisuuden periaatteen osalta skenaarion 3.2 mukainen käsittely aiheuttaisi rekisteröityjen oikeuksiin kohdistuvia riskejä, joita suunnitellut suojatoimet eivät lieventäisi. Hyvin monien henkilöiden pilvipalveluun tallennettuja biometrisia tietoja sisältävään keskitettyyn tietokantaan kohdistuvan tietoturvaloukkauksen mahdollisesti aiheuttama rekisteröityjen perusoikeuksiin ja -vapauksiin kohdistuva kielteinen vaikutus näyttäisi olevan suurempi kuin käsittelystä odotettavissa oleva hyöty, koska tällainen hyöty, eli tarkastusten lievä helpottuminen ja nopeutuminen, on suhteellisen vähäinen. Sen vuoksi tämä hyöty ei voi oikeuttaa tällaisia yksilöiden perusoikeuksiin ja -vapauksiin voimakkaasti puuttuvia toimenpiteitä eikä skenaarion 3.2 mukaista käsittelyä voida pitää oikeasuhteisena.

91. Näiden seikkojen perusteella tietosuojaneuvosto toteaa kysymyksen 2.3.1 osalta, että kun käsittely suoritetaan nimenomaisesti lentoasemien matkustajavirtojen sujuvoittamiseksi, skenaariossa 3.2 kaavailtu käsittely

- **ei voi olla yhteensopivaa yleisen tietosuoja-asetuksen 25 artiklan kanssa**
- **ei olisi yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan kanssa**, jos rekisterinpitäjä toteuttaisi vain skenaariossa 3.2 kuvatut toimenpiteet.
- **ei olisi yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan kanssa**, koska skenaariossa 3.2 tarkoitetulle säilytysajalle ei ole tietosuojaneuvoston käytettävissä olevien tietojen perusteella riittäviä perusteita. Noudattaakseen yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdassa säädettyä säilytyksen rajoittamisen periaatetta rekisterinpitäjän olisi osoitettava, että henkilötietoja ei säilytetä pidempään kuin on tarpeen niitä tarkoituksia varten, joita varten niitä käsitellään.

4 PÄÄTELMÄT

92. Kysymyksen 1.1 osalta tietosuojaneuvosto toteaa vastauksena Ranskan valvontaviranomaisen lausuntopyyntöön yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan sekä 25 ja 32 artiklan vaatimusten osalta edellä esitetyn analyysin perusteella seuraavaa:

93. Kasvontunnistusteknologian käytön biometriseen todentamiseen nimenomaisesti matkustajavirtojen sujuvoittamiseksi lentoasemilla (turvatarkastuspisteet, matkatavaroiden jättöpisteet, koneeseen siirtyminen ja matkustajien lounge-tilojen sisäänkäynnit) voidaan periaatteessa katsoa olevan yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan sekä 25 ja 32 artiklan mukaisten eheyden ja luottamuksellisuuden periaatteiden kanssa, jos kyseisessä tallennusrakenteessa kunkin matkustajan rekisteröity biometrinen malli säilytetään paikallisesti heidän henkilökohtaisella laitteellaan ja yksinomaan heidän valvonnassaan ja jos toteutetaan edellä 46 kohdassa kuvatut asianmukaiset suojatoimet.

94. Kysymyksen 2.1.1 osalta tietosuojaneuvosto toteaa vastauksena Ranskan valvontaviranomaisen lausuntopyyntöön yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan vaatimusten osalta edellä esitetyn analyysin perusteella seuraavaa:

95. Kasvontunnistusteknologian käytön biometriseen todennukseen nimenomaisesti matkustajavirtojen sujuvoittamiseksi lentoasemilla (turvatarkastuspisteet, matkatavaroiden jättöpisteet, koneeseen siirtyminen ja matkustajien lounge-tilojen sisäänkäynnit) voidaan periaatteessa katsoa olevan yhteensopivaa yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan mukaisen säilytyksen rajoittamisen periaatteen ja 5 artiklan 1 kohdan f alakohdan sekä 25 ja 32 artiklan mukaisten eheyden ja luottamuksellisuuden periaatteiden kanssa, jos kunkin matkustajan rekisteröity biometrinen malli säilytetään lentoasemalla sijaitsevassa keskitetyssä tallennusrakenteessa lentoaseman pitäjän valvonnassa salatussa muodossa, jonka avain/salasana on ainoastaan henkilön hallussa, ja jos toteutetaan edellä 60 kohdassa kuvatut asianmukaiset suojatoimet.

96. Kysymyksen 2.2.1 osalta tietosuojaneuvosto toteaa vastauksena Ranskan valvontaviranomaisen lausuntopyyntöön yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan vaatimusten osalta edellä esitetyn analyysin perusteella seuraavaa:

97. Kasvontunnistusteknologian käyttö biometriikkaan perustuvaan tunnistamiseen, jota käytetään nimenomaisesti matkustajavirtojen sujuvoittamiseksi lentoasemilla (turvatarkastuspisteet, matkatavaroiden jättöpisteet, koneeseen siirtyminen ja matkustajien lounge-tilojen sisäänkäynnit), ei voi olla yleisen tietosuoja-asetuksen 25 artiklan mukaista, jos käytetään keskitettyä tallennusrakennetta, jossa matkustajien rekisteröityjä biometrisiä malleja ei ole salattu yksinomaan kunkin matkustajan hallussa olevalla avaimella/salasanalla ja jos tällaisia malleja säilytetään lentoasemalla sijaitsevassa tietokannassa (lentoaseman pitäjän valvonnassa). Tällainen käsittely ei myöskään olisi yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan mukaisten eheyden ja luottamuksellisuuden periaatteiden mukaista, jos rekisterinpitäjä toteuttaisi vain skenaariossa 3.1 kuvatut toimenpiteet.

98. Kysymyksen 2.3.1 osalta tietosuojaneuvosto toteaa vastauksena Ranskan valvontaviranomaisen lausuntopyyntöön yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e ja f alakohdan sekä 25 ja 32 artiklan vaatimusten osalta edellä esitetyn analyysin perusteella seuraavaa:

99. Kasvontunnistusteknologian käyttö biometriikkaan perustuvaan tunnistamiseen, jota käytetään nimenomaisesti matkustajavirtojen sujuvoittamiseksi lentoasemilla (turvatarkastuspisteet, matkatavaroiden jättöpisteet, koneeseen siirtyminen ja matkustajien lounge-tilojen sisäänkäynnit), ei voi olla yleisen tietosuoja-asetuksen 25 artiklan mukaista, jos käytetään keskitettyä tallennusrakennetta, jossa matkustajien rekisteröityjä biometrisiä malleja ei ole salattu yksinomaan kunkin matkustajan hallussa olevalla avaimella/salasanalla ja jos tällaisia malleja säilytetään pilvipalvelussa (lentoyhtiön valvonnassa). Tällainen käsittely ei myöskään olisi yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan ja 32 artiklan mukaisten eheyden ja luottamuksellisuuden periaatteiden mukaista, jos rekisterinpitäjä toteuttaisi vain skenaariossa 3.2 kuvatut toimenpiteet. Skenaarion 3.2 kuvauksen ja tietosuojaneuvoston käytettävissä olevien tietojen perusteella käsittely ei myöskään olisi yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan mukaisen säilytyksen rajoittamisen periaatteen mukaista.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Anu Talus)