

Asia C-61/22

**Unionin tuomioistuimen työjärjestyksen 98 artiklan 1 kohdan mukainen
ennakkoratkaisupyynnön tiivistelmä**

Jättämispäivä:

1.2.2022

Ennakkoratkaisua pyytänyt tuomioistuin:

Verwaltungsgericht Wiesbaden (Wiesbadenin hallintotuomioistuin,
Saksa)

Ennakkoratkaisupyynnön esittämistä koskevan päätöksen tekemispäivä:

13.1.2022

Kantaja:

RL

Vastaaja:

Landeshauptstadt Wiesbaden

Pääasian kohde

Sormenjälkien ottaminen ja tallentaminen henkilökortteihin – Asetuksen (EU) 2019/1157 3 artiklan 5 kohta – Pätevyys – Asetuksen antamismenettely – Euroopan unionin perusoikeuskirjan 7 ja 8 artikla – Yleisen tietosuoja-asetuksen 35 artiklan 10 kohta

Ennakkoratkaisupyynnön kohde ja oikeusperusta

Asetuksen (EU) 2019/1157 3 artiklan 5 kohdan pätevyys, SEUT 267 artikla.

Ennakkoratkaisukysymys

Onko unionin kansalaisten henkilökorttien sekä oikeuttaan vapaaseen liikkuvuuteen käyttäville unionin kansalaisille ja heidän perheenjäsenilleen myönnettävien oleskeluasiakirjojen turvallisuuden lisäämisestä 20.6.2019 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1157 (EUVL L 188,

12.7.2019, s. 67) 3 artiklan 5 kohdassa säädetty velvollisuus ottaa sormenjäljet ja tallentaa ne henkilökortteihin ristiriidassa ylemmäntasoisien unionin oikeuden, erityisesti

- a) SEUT 77 artiklan 3 kohdan
 - b) Euroopan unionin perusoikeuskirjan 7 ja 8 artiklan
 - c) yleisen tietosuoja-asetuksen 35 artiklan 10 kohdan, kanssa
- ja siksi jonkin edellä mainitun perusteella pätemätön?

Unionin oikeussäännöt, joihin asiassa viitataan

Euroopan unionin perusoikeuskirja, 7, 8 ja 52 artikla

Sopimus Euroopan unionin toiminnasta (SEUT), 21, 77 ja 289 artikla

Unionin kansalaisten henkilökorttien sekä oikeuttaan vapaaseen liikkuvuuteen käyttäville unionin kansalaisille ja heidän perheenjäsenilleen myönnettävien oleskeluasiakirjojen turvallisuuden lisäämisestä 20.6.2019 annettu Euroopan parlamentin ja neuvoston asetus (EU) 2019/1157, johdanto-osan 2, 17, 18, 19, 21, 22, 40 ja 41 perustelukappale sekä 3 ja 11 artikla

Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annettu Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (yleinen tietosuoja-asetus), 9 ja 35 artikla

Kansalliset oikeussäännöt, joihin asiassa viitataan

Henkilökorteista ja sähköisestä henkilötodistuksesta annettu laki (Gesetz über Personalausweise und den elektronischen Identitätsnachweis, Personalausweisgesetz, jäljempänä PAuswG), 5 ja 9 §

Yhteenveto tosiseikoista ja menettelystä

- 1 Kantaja pyytää henkilökortin myöntämistä ilman sormenjälkien ottamista. Vastaja hylkäsi pyynnön, koska asetukseen (EU) 2019/1157 perustuvan henkilökorteista annetun lain (PAuswG) 5 §:n 9 momentissa vaaditaan kahden sormenjäljen ottamista.
- 2 Asetusta (EU) 2019/1157 on sovellettu 2.8.2021 alkaen. Asetuksen (EU) 2019/1157 3 artiklan 5 kohdassa säädetään, että jäsenvaltioiden myöntämiin henkilökortteihin on sisällyttävä tallennusväline, jossa on kortin haltijan kasvokuva ja kaksi sormenjälkeä yhteentoimivassa digitaalisessa muodossa. Myös

Saksan lainsäädännössä on säännöksiä sormenjälkien sisällyttämisestä henkilökortteihin (PAuswG 5 §:n 9 momentti), ja Saksan lainsäätäjä on lain perustelujen mukaan katsonut, että sormenjäljet on sisällytettävä henkilökorttiin asetuksen (EU) 2019/1157 3 artiklan 5 kohdan mukaisesti.

- 3 Kantaja haki 30.11.2021 uutta henkilökorttia ilman sormenjälkien ottamista, koska hänen vanhan henkilökorttinsa siru oli viallinen. Uuden henkilökortin myöntäminen evättiin, koska sormenjälkien ottaminen on ollut pakollista 2.8.2021 alkaen. Lisäksi todettiin, että kantajalla ei ollut oikeutta uuteen henkilökorttiin, koska hänellä oli jo voimassa oleva henkilötodistus. Henkilökortin todettiin olevan edelleen voimassa, vaikka siru oli viallinen.
- 4 Henkilökorttien myöntämisestä Saksan lainsäädännön mukaan vastuussa oleva viranomainen toimii turvallisuusviranomaisena. Henkilökorttien myöntämiseen ja siihen liittyvään tietojenkäsittelyyn ei kuitenkaan sovelleta direktiiviä (EU) 2016/680 vaan, kuten asetuksen (EU) 2019/1157 johdanto-osan 40 perustelukappaleesta käy ilmi, yleistä tietosuoja-asetusta. Nyt tarkasteltavassa asiassa ylipormestari ei näin ollen toimi unionin oikeuden itsenäisesti tulkittavan turvallisuuslainsäädännön alalla. Direktiivin (EU) 2016/680 1 artiklan 1 kohdan ja 2 artiklan 1 kohdan mukaan kyseistä direktiiviä sovelletaan ainoastaan silloin, kun viranomaiset toimivat rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten. Passi- ja henkilökorttijärjestelmä ei kuulu sen soveltamisalaan.

Yhteenveto ennakkoratkaisupyynnön perusteluista

- 5 Ennakkoratkaisukysymykseen annettava vastaus on välttämätön asian ratkaisemiseksi. Jos asetuksen (EU) 2019/1157 3 artiklan 5 kohta on ristiriidassa ylemmänasteisen unionin oikeuden kanssa, kantajalla on oikeus saada henkilökortti ilman sormenjälkien ottamista (PAuswG:n 9 §:n 1 momentin ensimmäinen virke). PAuswG:n 5 §:n 9 momenttiin sisältyvä kansallinen säännös menettäisi perusteensa, koska se olisi unionin oikeuden vastainen.
- 6 Vaikka kantajan vanha henkilökortti olisi viallisesta sirusta huolimatta edelleen voimassa PAuswG:n 28 §:n 3 momentin mukaisesti, kantajalle on myönnettävä uusi henkilökortti viimeistään kymmenvuotisen voimassaoloajan päättyttyä. Lisäksi PAuswG:n 6 §:n 2 momentin mukaan kantaja voi hakea uutta henkilökorttia ennen henkilökortin voimassaolon päättymistä, jos osoitetaan, että uuden henkilökortin myöntämiseen liittyy oikeutettu etu. Jos siru on viallinen, sähköisen tunnistustoiminnon käyttö ei ole enää mahdollista. Myöskään automaattista rajatarkastusta ei voida enää käyttää. Rajallisten käyttömahdollisuuksien vuoksi hakijalla on oikeutettu intressi uuteen henkilökorttiin.

- 7 Ennakkoratkaisua pyytäneellä tuomioistuimella on epäilyksiä siitä, onko asetuksen (EU) 2019/1157 3 artiklan 5 kohta unionin oikeuden mukainen. Nämä epäilyt perustuvat asetuksen (EU) 2019/1157 antamiseen tavallisessa lainsäätämisyjärjestyksessä, asetuksen (EU) 2019/1157 3 artiklan 5 kohdan yhteensopivuuteen Euroopan unionin perusoikeuskirjan (jäljempänä perusoikeuskirja) 7 ja 8 artiklan kanssa sekä yleisen tietosuoja-asetuksen 35 artiklan 10 kohdan mukaisen arviointipäätöksen puuttumiseen.
- 8 Kansallisen tuomioistuimen näkemyksen mukaan asetus (EU) 2019/1157 olisi pitänyt antaa SEUT 77 artiklassa tarkoitettua erityistä lainsäätämisyjärjestystä noudattaen.
- 9 SEUT 289 artiklassa erotetaan toisistaan tavallinen lainsäätämisyjärjestys ja erityiset lainsäätämisyjärjestykset. Asetuksen (EU) 2019/1157 perustana on SEUT 21 artiklan 2 kohta, ja se annettiin tavallista lainsäätämisyjärjestystä noudattaen. SEUT 21 artiklan 2 kohdan mukaan Euroopan parlamentti ja neuvosto voivat tavallista lainsäätämisyjärjestystä noudattaen antaa säännöksiä, joilla helpotetaan vapaata liikkuvuutta koskevan oikeutta käyttämistä, jos jokin unionin toimi osoittautuu tarpeelliseksi tämän tavoitteen saavuttamiseksi eikä perussopimuksissa ole määräyksiä tähän tarvittavista valtuuksista.
- 10 SEUT 77 artiklan 3 kohdan ensimmäiseen virkkeeseen sisältyy toinen toimivaltamääräys, joka koskee muun muassa henkilötodistuksia koskevia säännöksiä. Kyseisen määräyksen mukaan neuvosto voi antaa erityistä lainsäätämisyjärjestystä noudattaen säännöksiä, jotka koskevat passeja, henkilötodistuksia, oleskelulupia tai muita niihin rinnastettavia asiakirjoja, jos perussopimuksissa ei ole määräyksiä tähän tarvittavista valtuuksista ja jos unionin toimintaa tarvitaan helpottamaan mahdollisuutta käyttää oikeutta vapaaseen liikkuvuuteen. Neuvosto tekee ratkaisunsa yksimielisesti Euroopan parlamenttia kuultuaan. Tämä yksimielisyysvaatimus jättää jäsenvaltioille suuren itsemääräämisoikeuden tällä alalla.
- 11 SEUT 77 artikla vastaa entistä EY (EY:n perustamissopimuksen) 62 artiklaa. Lainsäätäjä tukeutui EY 62 artiklaan antaessaan asetuksen (EY) N:o 2252/2004, jonka 1 artiklan 2 kohdassa säädetään sormenjälkien tallentamisesta passeihin. Unionin tuomioistuin on katsonut 17.10.2013 antamassaan tuomiossa Schwarz (C-291/12, EU:C:2013:670), että EY 62 artiklan 2 kohdan a alakohda on asetuksen (EY) 2252/2004 ja etenkin sen 1 artiklan 2 kohdan antamisen asianmukainen oikeudellinen perusta.
- 12 SEUT 77 artiklan 3 kohdan mukainen toimivalta on etusijalla SEUT 21 artiklan 2 kohdan mukaiseen toimivaltaan nähden, koska SEUT 77 artiklan 3 kohdassa, joka on sisällöltään täsmällisempi määräys, asetetaan lainsäädäntömenettelylle tiukempia vaatimuksia, ja SEUT 21 artiklan 2 kohta on merkityksellinen vain, jos perussopimuksissa ei määrätä muista toimivaltuuksista vapaan liikkuvuuden edistämistä koskevan tavoitteen saavuttamiseksi. Vaikka asetuksessa (EU) 2019/1157 ei viitata Schengenin säännöstön kehittämiseen, sillä on asetuksen

(EY) N:o 2252/2004 tavoin tarkoitus yhdenmukaistaa turvaominaisuuksia ja sisällyttää niihin biometriset tunnisteet, mikä on tärkeä askel kohti tulevaa kehitystä ennakoivien uusien osien käyttöön ottamista Euroopan tasolla. Asetuksen (EY) N:o 2252/2004 tavoin myös sillä pyritään varmistamaan asiakirjojen turvallisuus (tässä kyse on henkilökorteista passien sijaan).

- 13 Kaiken edellä esitetyn perusteella kansallinen tuomioistuin katsoo, että asetuksen (EU) 2019/1157 – ja näin ollen myös kyseisen asetuksen 3 artiklan 5 kohdan – antaminen pätevästi olisi edellyttänyt SEUT 77 artiklan 3 kohdan mukaista erityistä lainsäätämistä.
- 14 Lisäksi sisällön osalta on epäilyksiä siitä, onko sormenjälkien ottaminen ja tallentaminen henkilökortteihin perusoikeuskirjan 7 ja 8 artiklan mukaista.
- 15 Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. Perusoikeuskirjan 8 artiklan mukaan jokaisella henkilöllä on oikeus henkilötietojensa suojaan.
- 16 Unionin tuomioistuin viittasi jo 17.10.2013 antamassaan tuomiossa Schwarz (C-291/12, EU:C:2013:670, 27 ja 30 kohta) Euroopan ihmisoikeustuomioistuimen 4.12.2008 antamaan tuomioon S. ja Marper v. Yhdistynyt kuningaskunta (Recueil des arrêts et décisions 2008-V, s. 213, 68 ja 84 kohta) ja totesi, että kansallisten viranomaisten menettelyllä, kun ne asetuksen N:o 2252/2004 1 artiklan 2 kohdassa säädetyn tavoin ottavat ja tallentavat sormenjäljet passeihin, loukataan oikeutta yksityiselämän kunnioittamiseen ja oikeutta henkilötietojen suojaan. Sormenjäljet ovat henkilötietoja, koska ne objektiivisesti sisältävät luonnollisia henkilöitä koskevia ainutkertaisia tietoja ja mahdollistavat heidän täsmällisen tunnistamisensa. Myös sormenjälkien ottamisessa ja tallentamisessa henkilökortteja varten on kyse samoista perusoikeuksista.
- 17 Kansallinen tuomioistuin on epävarma siitä, onko sormenjälkien ottaminen ja näin ollen puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin oikeuksiin perusteltua myös henkilökorttien tapauksessa, erityisesti kun otetaan huomioon perusoikeuskirjan 52 artikla ja 8 artiklan 2 kohta. Perusoikeuskirjan 8 artiklan 2 kohdassa vahvistetaan, että henkilötietoja voidaan käsitellä vain asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla.
- 18 Aivan kuten unionin tuomioistuin on todennut passeista, nyt tarkasteltavassa tapauksessa kansallinen tuomioistuin katsoo, että henkilökorttia hakevat henkilöt eivät ole antaneet suostumustaan sormenjäljen ottamiseen. Asetuksen (EU) 2019/1157 3 artiklan 5 kohtaan sisältyy kuitenkin sitä koskeva säännös, jota sovelletaan kaikkiin henkilökortteihin.
- 19 PAuswG:n 1 §:n 1 momentin ensimmäisen virkkeen mukaan kaikilta 16 vuotta täyttäneiltä saksalaisilta, jotka ovat yleisesti rekisteröintivelvollisia tai jotka eivät ole yleisesti rekisteröintivelvollisia mutta oleskelevat pääasiassa Saksassa, edellytetään voimassa olevaa henkilötodistusta. Sormenjälkien antaminen on näin

ollen pakollista tällaisen asiapaperin myöntämiseksi. Koska henkilökortti on pakollinen, henkilökorttia hakevien ei voida olettaa antaneen suostumustaan tällaiseen tietojenkäsittelyyn (ks. myös unionin tuomioistuimen tuomio 17.10.2013, Schwarz, C-291/12, EU:C:2013:670, 31 kohta).

- 20 Perusoikeuskirjan 52 artiklan 1 kohdan mukaan siihen tarvitaan näin ollen **hyväksyttävä** laissa säädetty perusta.
- 21 Sormenjälkien ottamisesta henkilökortteja varten säädetään asetuksen (EU) 2019/1157 3 artiklan 5 kohdassa. Tämä vastaa myös ainakin osittain unionin tunnustamia yleisen edun mukaisia tavoitteita, jotka on ilmaistu kyseisen asetuksen johdanto-osan 1, 2, 4, 18 ja 46 perustelukappaleissa.
- 22 Euroopan unionissa henkilökorttia voidaan käyttää rajanylityksessä. Lisäksi myös EU:hun kuulumattomat valtiot, erityisesti Sveitsi, Islanti, Norja, Albania ja Montenegro, sallivat maahantulon henkilökortilla. Tämän perusteella henkilökorttia käytetään ainakin myös matkustusasiakirjana, joten säännösten tavoitteena on myös estää laitton maahantulo näistä maista. Tällä pyritään unionin hyväksymään yleisen edun mukaiseen tavoitteeseen (tuomio 17.10.2013, Schwarz, C-291/12, EU:C:2013:670, 38 kohta). Henkilökorttia ei ole kuitenkaan tarkoitus käyttää pääasiallisesti matkustusasiakirjana Schengen-alueella, toisin kuin passia. Toisin kuin asetuksen (EU) N:o 2252/2004 johdanto-osan perustelukappaleissa, asetuksen (EU) 2019/1157 johdanto-osan perustelukappaleissa jätetään perustellusti viittaamatta Schengen-alueeseen vapauteen perustuvana alueena.
- 23 Asetuksessa (EU) 2019/1157 ei myöskään säännellä tallennettujen biometrinen tietojen käyttöä tämän osalta, sillä asetuksen (EU) 2019/1157 11 artiklan 6 kohdassa todetaan, että tallennettuja biometrisiä tietoja saa käyttää ainoastaan asiakirjan aitouden tai asiakirjan haltijan henkilöllisyyden todentamiseen. Asetuksessa (EU) 2019/1157 jätetään näin ollen avoimeksi, miten vapaata liikkuvuutta helpotetaan. Laittoman maahantulon estämisen tavoitetta ei voida tältä osin rinnastaa vapaan liikkuvuuden helpottamiseen.
- 24 Vaikka asetuksella pyritäisiinkin yleisen edun mukaiseen tavoitteeseen, on kuitenkin kyseenalaista, onko asetuksen (EU) 2019/1157 3 artiklan 5 kohta oikeasuhteinen. Näin olisi vain silloin, jos näille perusoikeuskirjan mukaisille oikeuksille asetetut rajoitukset ovat oikeassa suhteessa asetuksella (EU) 2019/1157 tavoiteltuihin päämääriin ja näin ollen siihen tavoitteeseen nähden, joka on estää henkilöiden laitton saapuminen unionin alueelle ja mahdollistaa asiakirjan haltijan henkilöllisyyden luotettava todentaminen. Asetuksella käyttöön otettujen keinojen on näin ollen sovellettava kyseisten tavoitteiden toteuttamiseen, eivätkä ne saa mennä pidemmälle kuin näiden tavoitteiden saavuttamiseksi on tarpeen (tuomio 17.10.2013, Schwarz, C-291/12, EU:C:2013:670, 38 ja 40 kohta).
- 25 Kansallisen tuomioistuimen näkemyksen mukaan tässä yhteydessä on otettava huomioon, että henkilökorttia ei voida tosiasiallisesti eikä oikeudellisesti rinnastaa

passiin, vaan näiden asiakirjojen käyttöön liittyy selviä eroja. Asetuksen (EU) 2019/1157 3 artiklan 5 kohdassa näitä kahta asiakirjaa kohdellaan kuitenkin sormenjälkien osalta yhdenmukaisesti.

- 26 Kuten edellä on jo todettu, henkilökorttia voidaan käyttää myös matkustusasiakirjana. Henkilökortit ja passit eroavat kuitenkin toisistaan sekä oikeudellisesti että käytännössä. Vaikka henkilökortteja käytetään myös matkustusasiakirjoina vapaan liikkuvuuden rajoissa, ainakaan EU:n jäsenvaltioiden välillä matkustettaessa ei tehdä rutiinitarkastuksia. Lisäksi useimpien unionin kansalaisten näkökulmasta kansallisen henkilökortin ensisijainen tarkoitus ei todennäköisesti liity vapaaseen liikkuvuuteen. Henkilökorteilla on nimittäin pidemmälle meneviä käyttötarkoituksia. Henkilökortteja käytetään arjessa esimerkiksi yhteydenpitoon kansallisten hallintoviranomaisten tai yksityisten kolmansien osapuolten, kuten pankkien tai lentoyhtiöiden, kanssa. Unionin kansalaiset, jotka haluavat käyttää oikeuttaan vapaaseen liikkuvuuteen, voivat tehdä sen jo nyt käyttämällä passiaan (ks. vastaavasti myös Euroopan tietosuoja-valtuutetun 10.8.2018 antama lausunto sormenjälkien suunnitellusta sisällyttämisestä henkilökortteihin).
- 27 Lisäksi PAuswG:n 1 §:n 1 momentin ensimmäisen virkkeen mukaan Saksassa henkilöiltä vaaditaan henkilökortti. Toisin kuin passin tapauksessa, kansalainen ei voi itse päättää, hakeeko hän henkilökorttia vai ei. Myös Euroopan tietosuoja-valtuutettu katsoo, että sormenjälkien ottamisella ja tallentamisella olisi laaja vaikutus jopa 370 miljoonaan EU:n kansalaiseen, ja vaatimus pakollisesta sormenjälkien ottamisesta voi mahdollisesti koskea 85:tä prosenttia EU:n väestöstä. Tämä laaja soveltamisala yhdistettynä erittäin arkaluonteisten tietojen (kasvokuvat yhdessä sormenjälkien kanssa) käsittelyyn edellyttää tarpeellisuuden arviointiin perustuvaa tarkkaa tarkastelua. Kansallinen tuomioistuin yhtyy Euroopan tietosuoja-valtuutetun näkemykseen siitä, että henkilökorttien ja passien välisten erojen vuoksi passeihin sopiviksi katsottavia turvaominaisuuksia ei voida ottaa automaattisesti käyttöön henkilökorteissa vaan niiden käyttöönotto vaatii harkintaa ja perusteellista analyysia. Tällaista ei ole vielä tehty.
- 28 Kansallinen tuomioistuin katsoo, että kun otetaan huomioon sekä edellä kuvatut laajat käyttömahdollisuudet että asianomaisten unionin kansalaisten suuri määrä, oikeuksiin puuttumisen aste on paljon korkeampi kuin passien tapauksessa, mikä puolestaan edellyttää myös vahvempia perusteluja.
- 29 Perusoikeuskirjan 7 ja 8 artiklaa tulkittaessa on otettava huomioon myös yleisessä tietosuoja-asetuksessa esitetyt toteamukset, jotka käyvät ilmi sen johdanto-osan ensimmäisestä ja toisesta perustelukappaleesta.
- 30 Sormenjälkitiedot ovat yleisen tietosuoja-asetuksen 9 artiklan 1 alakohdan mukaisia erityisiä henkilötietoja eli biometrisiä tietoja. Yleisen tietosuoja-asetuksen 4 artiklan 14 kohdan mukaan biometrisillä tiedoilla tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai

sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa. Yleisen tietosuoja-asetuksen 9 artiklan 1 kohdan mukaan tällaisten biometristen tietojen käsittely on lähtökohtaisesti kiellettyä, ja se sallitaan vain poikkeustapauksissa.

- 31 Siltä osin kuin sormenjäljet olisi sisällytettävä henkilökortteihin niiden suojaamiseksi väärennysiltä, Euroopan tietosuojavaltuutetun lausunnossa todetaan sormenjälkikuvien suunnitellusta tallentamisesta henkilökortteihin, että vuosina 2013–2017 havaittiin vain 38 870 väärennettyä henkilötodistusta ja että väärennettyjen henkilötodistusten käyttö on vähentynyt jo vuosia.
- 32 Vielä ei ole riittävän selvää, voidaanko sormenjälkien ottamisella tosiasiaa edistää väärennössuojausta. Henkilökortin mikrosirulle tallennettujen biometristen tietojen ja kortin haltijan sormenjälkien välisellä vastaavuudella vahvistetaan ainoastaan, että asiakirja kuuluu haltijalle. Vastaavuus sinänsä ei ole todiste henkilöllisyydestä, jos itse henkilökorttia ei ole todettu aidoksi. On kuitenkin tunnustettu, että biometristen tietojen käyttö vähentää asiakirjan onnistuneen väärentämisen todennäköisyyttä, joten sormenjälkien ottamisella voidaan ainakin osittain edistää tätä tarkoitusta.
- 33 On kuitenkin hyvin kyseenalaista, voidaanko tällä mahdollisuudella perustella laajaa puuttumista oikeuksiin, varsinkin koska Saksan lainsäädännön mukaan myös viallisen sirun sisältävä henkilökortti on edelleen voimassa vastoin asetusta (EU) 2019/1157. Bundesamt für Sicherheit in der Informationstechnik (Saksan liittovaltion tietoturvavirasto) toteaa tältä osin, että ”henkilökortti, jossa on toimimaton siru, [on edelleen] voimassa, vaikka integroitu siru olisikin tunnistettavasti viallinen. Henkilötodistuksen turvallisuus perustuu fyysisiin turvaominaisuuksiin”. Jos turvallisuus kuitenkin varmistetaan yksistään fyysisillä turvaominaisuuksilla (erityisesti mikrokirjoitukset, UV-painatukset jne.), sormenjälkien ottamisen tarpeellisuutta koskeva kysymys nousee sitäkin selvemmin esiin.
- 34 Myös Euroopan tietosuojavaltuutettu on korostanut, että asiakirjan painamiseen liittyvät turvatoimenpiteet, kuten hologrammien tai vesileimojen käyttö, olisivat paljon lievempiä toimenpiteitä. Nämä menetelmät eivät edellyttäisi henkilötietojen käsittelyä, mutta niiden avulla voitaisiin myös estää henkilötodistusten väärentäminen ja todentaa asiakirjan aitous.
- 35 Tässä yhteydessä on myös noudatettava yhtä EU:n tietosuojalainsäädännön tärkeimmistä periaatteista eli tietojen minimointia koskevaa periaatetta. Sen mukaan henkilötietojen keräämisen ja käytön on oltava oikeasuhteista ja tarpeellista ja rajoituttava siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten tietoja käsitellään.
- 36 Jos on tarpeen ottaa sormenjäljet, herää myös kysymys, miksi on tarpeen ottaa koko sormenjälkikuva. Tällä edistetään kuitenkin sormenjälkien tunnistamiseen käytettävien erityyppisten järjestelmien yhteentoimivuutta. Tällaiset järjestelmät

voidaan jakaa kolmeen alaluokkaan. Ensinnäkin on järjestelmiä, jotka tallentavat ja vertailevat koko sormenjälkikuvaa. Toiset järjestelmät käyttävät erikoiskohdista otettuja kuvia. Nämä erikoiskohdat ilmentävät osaa sormenjälkikuvasta saaduista piirteistä. Kolmanteen luokkaan kuuluvat järjestelmät, jotka toimivat sormenjälkikuvista poimittujen yksittäisten kuvioiden avulla. Jos tallennettaisiin vain sormenjäljessä oleva erikoiskohta, jäsenvaltio, jolla on käytössä koko sormenjälkikuvaa hyödyntävä järjestelmä, ei voisi käyttää sitä. Koko sormenjälkikuvan tallentaminen parantaa yhteentoimivuutta, mutta tällöin tallennettujen henkilötietojen määrä ja samalla identiteettivarkauden riski kasvaa tietovuodon sattuessa.

- 37 Henkilökorteissa käytetyt RFID-sirut voidaan tietyissä olosuhteissa lukea myös luvattomilla skannereilla. Tämä johtuu siitä, että ne aktivoituvat radiokentän avulla ja välittävät sen jälkeen tiedot salatussa muodossa. Menettelyn turvallisuus riippuu näin ollen viime kädessä tiedonsiirto- ja salaustekniikan laadusta. Koko sormenjälkikuvan käyttö lisää tässä yhteydessä riskiä.
- 38 Tällöin on myös huomattava, että sormenjäljet ovat biometrisiä tietoja. Lainsäätäjä on muun muassa yleisen tietosuoja-asetuksen 9 artiklaa säätäessään osoittanut, että ne ovat erityisen suojelun kohteena.
- 39 Myös asetuksessa (EU) 2019/1157 luovutaan sormenjälkien ”turvaominaisuudesta” alle 12-vuotiaiden lasten osalta ja vapautetaan alle 6-vuotiaat lapset kokonaan sormenjälkien antamista koskevasta velvollisuudesta, ks. asetuksen (EU) 2019/1157 3 artiklan 7 kohta. Vielä tärkeämpää on kuitenkin se, että henkilöihin, jotka eivät fyysisten rajoitteiden vuoksi pysty antamaan sormenjälkiä, ei sovelleta sormenjälkien antamista koskevaa vaatimusta. Siitä, mitä tällä turvaominaisuudella sitten tavoitellaan, ei säädetä asetuksessa (EU) 2019/1157, ja se jää yksinkertaisesti avoimeksi.
- 40 Euroopan tietosuojavaltuutettu on korostanut lausunnossaan myös, että yleisen tietosuoja-asetuksen 35 artiklan 10 kohtaa sovelletaan sormenjälkien ottamiseen ja käsittelyyn. Yleisen tietosuoja-asetuksen 35 artiklan 1 kohdan mukaan tietosuoja koskeva vaikutustenarviointi on tehtävä ennen käsittelyä, jos se todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Tässä tietosuoja koskevassa vaikutustenarvioinnissa olisi erityisesti arvioitava rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä ja näiden riskien torjumiseksi toteutettavia toimenpiteitä, kuten suoja- ja turvallisuustoimia.
- 41 Koska käsittelyn oikeusperusteena on rekisterinpitäjään sovellettava unionin oikeus, jolla säännellään siihen liittyvää käsittelytointa, yleinen vaikutustenarviointi on tehtävä tämän oikeusperusteen hyväksymisen yhteydessä (yleisen tietosuoja-asetuksen 35 artiklan 10 kohta). Tällainen vaikutustenarviointi olisi sen vuoksi pitänyt tehdä, kun asetus (EU) 2019/1157 annettiin. Johdanto-osan perustelukappaleiden mukaan näin ei ole tehty.

- 42 Kansallinen tuomioistuin yhtyy tietosuojavaltuutetun lausunnossaan esittämään näkemykseen siitä, että vaikutustenarviointi ei tue sekä kasvokuvien että (kahden) sormenjälkikuvan pakollista sisällyttämistä henkilökortteihin. Euroopan tietosuojavaltuutettu suositteli jo lainsäädäntömenettelyn aikana, että biometristen tietojen (kasvokuva yhdessä sormenjälkien kanssa) käsittelyn tarpeellisuutta ja oikeasuhteisuutta arvioitaisiin uudelleen tässä yhteydessä.
- 43 Lainsäätäjä tarkastelee tätä ongelmaa vain hyvin yleisesti yleisen tietosuojasetuksen osalta sen 40 perustelukappaleessa. Se on esittänyt epämääräisiä lausumia muun muassa siitä, että unionin kansalaisten olisi saatava tietoa tallennusvälineestä ja että olisi täsmennettävä, mitä suojatoimia sovelletaan käsiteltyihin henkilötietoihin ja erityisesti arkaluonteisiin tietoihin, kuten biometrisiin tunnistuksiin. Tallennusvälineen olisi oltava erittäin turvallinen ja suojattava siihen tallennetut henkilötiedot tehokkaasti luvattomalta pääsylvä. On epäselvää, mitä tarkoitetaan ”erittäin turvallisella” ja miten suoja- ja turvallisuustoimet on toteutettava. Nähtävissä ei ole etenkin, että asiaa olisi punnittu mikrosirun tietovuodon riskien ja perusoikeuskirjan 7 ja 8 artiklan rikkomisen kannalta.
- 44 Näin ollen herää kysymys, voiko pakollisen riskejä koskevan vaikutustenarvioinnin tekemättä jättäminen olla vaikuttamatta oikeussäännön tehokkuuteen vai onko pikemminkin niin, että sen tekemättä jättäminen johtaa oikeussäännön pätemättömyyteen, jos lainsäätäjä on velvollinen tekemään riskejä koskevan vaikutustenarvioinnin. Muussa tapauksessa lainsäätäjää palkittaisiin sen virheellisestä toiminnasta.