

Mål C-61/22

Sammanfattning av begäran om förhandsavgörande enligt artikel 98.1 i domstolens rättegångsregler

Datum för ingivande:

1 februari 2022

Domstol som begär förhandsavgörande:

Verwaltungsgericht Wiesbaden (Tyskland)

Datum för beslutet att begära förhandsavgörande:

13 januari 2022

Klagande:

RL

Motpart:

Landeshauptstadt Wiesbaden

Saken i det nationella målet

Införande och lagring av fingeravtryck i identitetskort – Artikel 3.5 i förordning (EU) 2019/1157 – Giltighet – Förfarandet för antagande av förordningen – Artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna – Artikel 35.10 i den allmänna dataskyddsförordningen

Syfte med och rättslig grund för begäran om förhandsavgörande

Giltigheten av artikel 3.5 i förordning (EU) 2019/1157, artikel 267 FEUF

Fråga som har hänskjutits för förhandsavgörande

Ska skyldigheten att införa och lagra fingeravtryck i identitetskort enligt artikel 3.5 i Europaparlamentets och rådets förordning (EU) 2019/1157 av den 20 juni 2019 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar

rätten till fri rörlighet (EUT L 188, 2019, s. 67) anses strida mot överordnad unionsrätt, i synnerhet

- a) mot artikel 77.3 FEUF
 - b) mot artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna
 - c) mot artikel 35.10 i den allmänna dataskyddsförordningen
- och därmed anses vara ogiltig på någon av dessa grunder?

Anförda unionsbestämmelser

Europeiska unionens stadga om de grundläggande rättigheterna: artiklarna 7, 8 och 52.

Fördraget om Europeiska unionens funktionssätt: artiklarna 21, 77 och 289.

Europaparlamentets och rådets förordning (EU) 2019/1157 av den 20 juni 2019 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet: skälen 2, 17, 18, 19, 21, 22, 40 och 41, samt artiklarna 3 och 11.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning): artiklarna 9, 35

Anförda nationella bestämmelser

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz – PAuswG) (lagen om identitetskort och elektronisk identifiering: 5 och 9 §§.

Kortfattad redogörelse för de faktiska omständigheterna och förfarandet i det nationella målet

- 1 Klaganden, RL, har begärt att ett identitetskort ska utfärdas utan införande av fingeravtryck. Motparten, Landeshauptstadt Wiesbaden, har avslagit begäran, eftersom 5 § stycke 9 i Personalausweisgesetz (nedan kallad PAuswG), som grundas på förordning (EU) 2019/1157, innehåller ett obligatoriskt krav på införande av två fingeravtryck i identitetskort.
- 2 Förordning (EU) 2019/1157 trädde i kraft den 2 augusti 2021. Artikel 3.5 i förordning (EU) 2019/1157 föreskriver att identitetskort som utfärdas av

medlemsstaterna ska innefatta ett lagringsmedium som innehåller en ansiktsbild av innehavaren och två fingeravtryck i interoperabla digitala format. Bestämmelser om införande av fingeravtryck i identitetskort har även införts i tysk lagstiftning (5 § stycke 9 PAuswG). Det framgår av förarbetena till nämnda lag att den tyska lagstiftaren ansett att artikel 3.5 i förordning (EU) 2019/1157 innebär ett krav på införande av fingeravtryck i identitetskort.

- 3 Den 30 november 2021 ansökte RL om utfärdande av ett nytt identitetskort utan fingeravtryck, eftersom chipet i hans gamla identitetskort var sönder. Landeshauptstadt Wiesbaden nekade att utfärda ett nytt identitetskort, eftersom införande av fingeravtryck i identitetskort är obligatoriskt sedan den 2 augusti 2021. Dessutom ansåg Landeshauptstadt Wiesbaden att RL inte hade någon rätt att erhålla ett nytt identitetskort, eftersom han redan har en giltig identitetshandling. Ett identitetskort är fortfarande giltigt, även om chipet är sönder.
- 4 Myndigheten som är ansvarig för att utfärda identitetskort agerar i egenskap av en myndighet som förhindrar hot mot den allmänna säkerheten. Trots detta omfattas utfärdande av identitetskort och den tillhörande databehandlingen inte av direktiv (EU) 2016/680, utan – som framgår av skäl 40 i förordning (EU) 2019/1157 – av den allmänna dataskyddsförordningen. I förevarande fall agerar Oberbürgermeister således inte på området för den unionsrättsliga lagstiftningen som syftar till att förhindra hot mot den allmänna säkerheten, vilken ska ges en självständig tolkning. Enligt artiklarna 1.1 och 2.1 i direktiv (EU) 2016/680 ska detta direktiv endast tillämpas för åtgärder som vidtas av myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Utfärdande av pass och identitetshandlingar är inte en sådan åtgärd.

Kortfattad redogörelse för skälen till att förhandsavgörande begärs

- 5 Det krävs ett svar på tolkningsfrågan för att den hänskjutande domstolen ska kunna döma i saken. Om artikel 3.5 i förordning (EU) 2019/1157 strider mot överordnad unionslagstiftning har RL rätt att få ett identitetskort utfärdat utan införande av fingeravtryck, 9 § stycke 1 första meningen PAuswG. Den nationella bestämmelsen i 5 § stycke 9 PAuswG skulle förlora sin rättsliga grund, då den skulle strida mot unionsrätten.
- 6 Även om RL:s gamla identitetskort fortfarande är giltigt enligt 28 § stycke 3 PAuswG trots att chipet är sönder, är RL skyldig att ansöka om ett nytt identitetskort senast när giltighetstiden på tio år har löpt ut. Dessutom har RL rätt att ansöka om ett nytt identitetskort enligt 6 § stycke 2 PAuswG innan det gamla har upphört att gälla om det finns ett berättigat intresse av att ett nytt identitetskort utfärdas. Om chipet är sönder är det inte längre möjligt att använda funktionen för online-identifiering. Det är inte heller möjligt att använda automatiska

gränskontroller utan chip. Dessa begränsade användningsmöjligheter innebär att det föreligger ett berättigat intresse av att ett nytt identitetskort utfärdas.

- 7 Den hänskjutande domstolen är osäker på huruvida artikel 3.5 i förordning (EU) 2019/1175 är förenlig med unionsrätten. Denna osäkerhet grundas på att förordning (EU) 2019/1157 antogs enligt det ordinarie lagstiftningsförfarandet, på frågan huruvida artikel 3.5 i förordning (EU) 2019/1157 är förenlig med artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan) och på omständigheten att en konsekvensbedömning inte genomförts i enlighet med artikel 35.10 i den allmänna dataskyddsförordningen.
- 8 Den hänskjutande domstolen anser att förordning (EU) 2019/1157 borde ha antagits inom ramen för det särskilda lagstiftningsförfarandet enligt artikel 77 FEUF.
- 9 I artikel 289 FEUF görs en åtskillnad mellan det ordinarie lagstiftningsförfarandet och särskilda lagstiftningsförfaranden. Förordning (EU) 2019/1157 grundades på artikel 21.2 FEUF och antogs inom ramen för det ordinarie lagstiftningsförfarandet. Enligt artikel 21.2 FEUF får Europaparlamentet och rådet i enlighet med det ordinarie lagstiftningsförfarandet anta bestämmelser i syfte att underlätta utövandet av rätten till fri rörlighet, om en åtgärd från unionens sida är nödvändig för att uppnå detta mål och om inte befogenheter för detta föreskrivs i fördragen.
- 10 Artikel 77.3 första meningen FEUF innehåller en ytterligare kompetensnorm som bland annat rör bestämmelser om identitetskort. Enligt nämnda bestämmelse får rådet i enlighet med ett särskilt lagstiftningsförfarande anta bestämmelser om pass, identitetskort, bevis om uppehållstillstånd eller andra jämförbara dokument, om befogenheter för detta ändamål inte föreskrivs i fördragen och om en åtgärd från unionens sida är nödvändig för att underlätta utövandet av rätten till fri rörlighet. Rådet ska besluta med enhällighet efter att ha hört Europaparlamentet. Kravet på enhällighet garanterar att medlemsstaterna har största möjliga självbestämmande på detta område.
- 11 Artikel 77 FEUF motsvarar den tidigare artikel 62 i EG-fördraget. Förordning (EG) [nr] 2252/2004, vars artikel 1.2 föreskriver att fingeravtryck ska lagras i pass, antogs av lagstiftaren med stöd av artikel 62 EG. EU-domstolen fastslog i domen av den 17 oktober 2013, Schwarz (C-291/12, EU:C:2013:670) att artikel 62 led 2 a EG utgjorde en lämplig rättslig grund för att anta förordning nr 2252/2004 och särskilt artikel 1.2 i samma förordning.
- 12 Befogenheten enligt artikel 77.3 FEUF har företräde framför artikel 21.2 FEUF, eftersom artikel 77.3 FEUF till sitt innehåll är en mer speciell bestämmelse som ställer högre krav på lagstiftningsförfarandet, medan artikel 21.2 FEUF endast är tillämplig om befogenheter inte föreskrivs i fördragen för att uppnå målet att främja den fria rörligheten. Förordning (EU) 2019/1157 rör visserligen inte vidareutvecklingen av Schengenregelverket, men syftar i likhet med förordning

(EG) [nr] 2252/2004 till harmoniseringen av säkerhetsdetaljer och införandet av biometriska kännetecken som ett viktigt steg på vägen mot användandet av nya element, med tanke på framtida utveckling på europeisk nivå. Målet är, i likhet med målet för förordning (EG) [nr] 2252/2004, att göra identitetshandlingar (i detta fall identitetskort i stället för pass) säkrare.

- 13 Mot bakgrund av det ovan anförda anser den hänskjutande domstolen att det var nödvändigt att tillämpa det särskilda lagstiftningsförfarandet enligt artikel 77.3 FEUF för att anta förordning (EU) 2019/1157 – och därmed även artikel 3.5 i förordningen – med giltig verkan.
- 14 Dessutom är det tveksamt huruvida åtgärder för upptagande och lagring av fingeravtryck på identitetskort i materiellt hänseende är förenliga med artiklarna 7 och 8 i stadgan.
- 15 Enligt artikel 7 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Artikel 8 i stadgan föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
- 16 EU-domstolen fastslog redan i domen av den 17 oktober 2013, Schwarz (C-291/12, EU:C:2013:670, punkterna 27 och 30) med hänvisning till Europadomstolens dom av den 4 december 2008 i målet S. och Marper mot Förenade kungariket, Recueil des arrêts et décisions 2008-V, s. 213, punkterna 68 och 84) att nationella myndigheters upptagande och lagring av fingeravtryck i pass, i enlighet med artikel 1.2 i förordning nr 2252/2004, innebär ett intrång i respekten för privatlivet och skyddet för personuppgifter. Fingeravtryck är personuppgifter, eftersom de objektivt sett innehåller unika uppgifter om fysiska personer och gör det möjligt att exakt identifiera dem. Samma grundläggande rättigheter berörs även vid upptagande och lagring av fingeravtryck med avseende på identitetskort.
- 17 Den hänskjutande domstolen är osäker på huruvida upptagande av fingeravtryck – och därmed ett ingrepp i rättigheterna enligt artiklarna 7 och 8 i stadgan, i synnerhet med hänsyn till artikel 52 och artikel 8.2 i stadgan – är rättfärdigat även med avseende på identitetskort. Artikel 8.2 i stadgan föreskriver att personuppgifter endast får behandlas på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund.
- 18 I det nu aktuella målet anser den hänskjutande domstolen – i likhet med vad EU-domstolen har konstaterat avseende pass – att den som ansöker om identitetskort inte har lämnat sitt samtycke till upptagande av fingeravtryck. Artikel 3.5 i förordning (EU) 2019/1157 är emellertid en lagbestämmelse som föreskriver detta för alla identitetskort.
- 19 Enligt 1 § stycke 1 första meningen PAuswG är alla tyskar skyldiga att inneha en giltig identitetshandling från och med att de fyllt 16 år och om de omfattas av den allmänna folkbokföringsskyldigheten, eller, om de inte omfattas av denna skyldighet, till övervägande del är bosatta i Tyskland. Det är obligatoriskt att

lämna fingeravtryck för att en sådan handling ska utfärdas. Eftersom det finns en skyldighet att inneha en identitetshandling kan en person som ansöker om ett identitetskort inte anses ha lämnat sitt samtycke till sådan behandling av personuppgifter (detta slogs fast av EU-domstolen i dom av den 17 oktober 2013, Schwarz, C-291/12, EU:C:2013:670, punkt 31).

- 20 Enligt artikel 52.1 i stadgan krävs således en **legitim** rättslig grund.
- 21 Artikel 3.5 i förordning (EU) 2019/1157 är visserligen en lagstadgad föreskrift som innebär att fingeravtryck ska införas. Detta överensstämmer åtminstone delvis med mål av allmänt samhällsintresse som erkänns i unionen, såsom dessa kommer till uttryck i skälen 1, 2, 4, 18 och 46.
- 22 Inom Europeiska unionen kan identitetskort användas vid gränsövergångar. Dessutom tillåter även stater som inte tillhör EU inresa med identitetskort, bland andra Schweiz, Island, Norge, Albanien och Montenegro. Mot denna bakgrund används identitetskort under alla omständigheter också som en resehandling, vilket innebär att bestämmelsen även har till syfte att förhindra illegal inresa från dessa länder. Detta är ett mål av allmänt samhällsintresse som erkänns av unionen (EU-domstolen, dom av den 17 oktober 2013, Schwarz, C-291/12, EU:C:2013:670, punkt 38). Huvudsyftet med ett identitetskort är emellertid inte i första hand att utgöra en resehandling i Schengenområdet på samma sätt som ett pass. I det avseendet hänvisar skälen i förordning (EU) 2019/1157 – i motsats till skälen i förordning nr 2252/2004 – helt riktigt inte till Schengenområdet som ett område med frihet.
- 23 I förordning (EU) 2019/1157 regleras användningen av lagrade biometriska uppgifter inte heller i detta avseende, då artikel 11.6 i förordning (EU) 2019/1157 föreskriver att biometriska uppgifter som lagrats bara får användas i syfte att kontrollera identitetskortets äkthet eller innehavarens identitet. I förordning (EU) 2019/1157 lämnas alltså frågan hur den fria rörligheten ska underlättas obesvarad. Målet att förhindra illegal inresa kan således inte likställas med att underlätta den fria rörligheten.
- 24 Även om bestämmelsen syftar till att uppnå ett mål av allmänt samhällsintresse är det emellertid oklart huruvida artikel 3.5 i förordning (EU) 2019/1157 är proportionerlig. Det skulle endast vara fallet om de begränsningar som har gjorts av rättigheter enligt stadgan är proportionerliga med hänsyn till de syften som eftersträvas i förordning (EU) 2019/1157 och således syftet att hindra att personer inreser olagligen till unionen och att möjliggöra tillförlitlig identifiering av innehavaren av identitetshandlingen. För att detta krav ska vara uppfyllt måste de medel som föreskrivs i förordningen vara ägnade att säkerställa att de syften som eftersträvas uppnås och att de inte går utöver vad som är nödvändigt för att uppnå dessa syften (EU-domstolen, dom av den 17 oktober 2013, Schwarz, C-291/12, EU:C:2013:670, punkterna 38 och 40).

- 25 Den hänskjutande domstolen anser att det i detta sammanhang är nödvändigt att ta hänsyn till att identitetskort i faktiskt och rättsligt hänseende inte kan likställas med pass, utan att det finns betydande skillnader när det gäller användningen av dessa handlingar. Trots detta likställs båda dessa handlingar när det gäller fingeravtryck enligt artikel 3.5 i förordning (EU) 2019/1157.
- 26 Visserligen kan identitetskort – som redan konstaterats ovan – även användas som resehandling. Trots detta skiljer sig identitetskort från pass i både rättsligt och praktiskt hänseende. Även om identitetskort också kan användas som resehandling inom ramen för den fria rörligheten sker inga rutinkontroller, i vart fall inte vid resor mellan EU-medlemsstater. Dessutom torde den huvudsakliga funktionen med det nationella identitetskortet för de flesta unionsmedborgare inte vara förknippad med den fria rörligheten. Identitetskort har nämligen användningsområden som går utöver detta. Till vardags används identitetskort bland annat vid kontakt med nationella myndigheter eller med privata aktörer som banker eller flygbolag. Unionsmedborgare som vill utöva sin fria rörlighet kan redan göra det med sitt pass (se, för ett liknande resonemang, även den Europeiska datatillsynsmannens yttrande rörande det planerade införandet av lagring av fingeravtryck i identitetskort av den 10 augusti 2018).
- 27 I Tyskland finns dessutom en skyldighet att inneha ett identitetskort enligt 1 § stycke 1 första meningen PAuswG. Medborgare kan, till skillnad från ett pass, inte själva välja om de ska ansöka om ett identitetskort eller inte. Även den Europeiska datatillsynsmannen anser att integrering och lagring av fingeravtryck skulle ha en omfattande inverkan på upp till 370 miljoner EU-medborgare, eftersom 85 procent av EU:s befolkning potentiellt skulle omfattas av det obligatoriska kravet på fingeravtryck. Denna vida räckvidd i kombination med de mycket känsliga uppgifter som behandlas (ansiktsbilder i kombination med fingeravtryck) kräver en mycket ingående granskning av huruvida detta är strikt nödvändigt. Den hänskjutande domstolen delar den Europeiska datatillsynsmannens resonemang att säkerhetsdetaljer som kan anses lämpliga för pass, med beaktande av skillnaderna mellan identitetskort och pass, inte automatiskt kan införas vad gäller identitetskort, utan detta behöver diskuteras och bedömas noggrant. Det har inte skett i förevarande fall.
- 28 Den hänskjutande domstolen anser att kombinationen av det ovannämnda vida användningsområdet och det stora antalet unionsmedborgare som påverkas medför ett mycket större intrång i jämförelse med pass, vilket även ställer krav på en mer kraftfull motivering av åtgärderna.
- 29 Inom ramen för tolkningen av artiklarna 7 och 8 i stadgan ska även principerna i den allmänna dataskyddsförordningen, såsom dessa framgår av skälen 1 och 2 i samma förordning, beaktas.
- 30 Fingeravtrycksuppgifter hör till en särskild kategori av personuppgifter enligt artikel 9.1 i den allmänna dataskyddsförordningen, nämligen biometrisk datauppgifter. I artikel 4 punkt 14 i den allmänna dataskyddsförordningen definieras

dessas som personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter. Enligt artikel 9.1 den allmänna dataskyddsförordningen är behandling av sådana uppgifter i princip förbjuden och endast tillåten i restriktivt definierade undantagsfall.

- 31 I den mån införande av fingeravtryck i identitetskort har till syfte att stärka skyddet mot förfalskning, har den Europeiska datatillsynsmannens i sitt yttrande angett att endast 38 870 förfalskade identitetskort ska ha konstaterats under åren 2013–2017 och att användningen av förfalskade identitetskort har avtagit under flera års tid.
- 32 Det framgår inte tillräckligt tydligt huruvida införande av fingeravtryck i identitetskort ökar skyddet mot förfalskning. Att de biometriska uppgifterna som lagrats på chipet överensstämmer med fingeravtrycken hos personen som innehar identitetskortet bekräftar endast att handlingen tillhör innehavaren. Överensstämmelsen i sig styrker dock inte identiteten, så länge identitetskortet i sig inte fastställs vara äkta. Det är visserligen erkänt att användningen av biometriska uppgifter minskar sannolikheten att en handling förfalskas med framgång, vilket innebär att en åtgärd för att ta fingeravtryck åtminstone delvis kan främja detta syfte.
- 33 Det framstår dock som högst tveksamt om denna möjlighet kan rättfärdiga ett så omfattande ingrepp, i synnerhet då även ett identitetskort med defekt chip fortfarande är giltigt enligt tysk rätt, i strid med förordning (EU) 2019/1157. I detta sammanhang har den tyska it-säkerhetsmyndigheten "Bundesamt für Sicherheit in der Informationstechnik" angett att "ett identitetskort med ett chip som inte fungerar fortsätter att vara giltigt, även om det är tydligt att chipet är sönder. De fysiska säkerhetsdetaljerna garanterar säkerheten hos identitetshandlingen." När säkerheten emellertid redan garanteras av de fysiska säkerhetsdetaljerna (mikrotext, UV-tryck, och så vidare) kan det i än högre grad ifrågasättas varför det är nödvändigt att införa fingeravtryck i identitetskort.
- 34 Även den Europeiska datatillsynsmannen betonade att säkerhetsåtgärder som avser handlingarnas tryck, såsom användning av hologram eller vattenmärken, är betydligt mindre ingripande åtgärder. Dessa metoder omfattar ingen behandling av personuppgifter, men förmår ändå hindra förfalskning av identitetshandlingar och verifiera äktheten hos en handling.
- 35 I detta sammanhang ska även en av de viktigaste principerna i den europeiska dataskyddslagstiftningen beaktas: principen om uppgiftsminimering eller dataminimering. Denna princip innebär att insamling och användning av personuppgifter ska vara proportionell, nödvändig och begränsad till vad som är nödvändigt för att uppnå målen med behandlingen.

- 36 Om det skulle vara nödvändigt med upptagande av fingeravtryck uppkommer dessutom frågan varför det är nödvändigt med en avbildning av hela fingeravtrycket. Härigenom främjas visserligen interoperabilitet mellan olika typer av system som kan läsa fingeravtryck. Dessa system kan indelas i tre underkategorier. För det första finns system som lagrar och jämför avbildningar av hela fingeravtryck. Andra system använder i stället detaljer av fingeravtryck. Dessa detaljer utgör en delmängd av de kännetecken som hämtas från fingeravtrycksbilderna. Den tredje kategorin är system som använder sig av avbildningar av enskilda mönster som hämtas från fingeravtrycken. Om endast en detalj av fingeravtrycket lagras kan en medlemsstat som arbetar med ett system som använder hela fingeravtrycket inte använda denna detaljbild. Lagring av hela fingeravtrycket främjar interoperabilitet, men ökar samtidigt mängden lagrade personuppgifter och därmed risken för identitetsstöld vid en eventuell dataläcka.
- 37 De RFID-chip som används i identitetskort kan under vissa omständigheter inte läsas av auktoriserade RFID-läsare. Det beror på att chipen aktiveras via radiolänk och därefter överför uppgifterna i krypterad form. Därmed är förfarandets säkerhet i slutändan beroende av kvaliteten på överförings- och krypteringstekniken som används. Användningen av hela fingeravtrycket ökar riskerna i detta sammanhang.
- 38 I sammanhanget ska det även beaktas att fingeravtryck är biometriska uppgifter. Lagstiftaren har bland annat genom införandet av artikel 9 i den allmänna dataskyddsförordningen visat att dessa ska omfattas av ett särskilt skydd.
- 39 Enligt förordning (EU) 2019/1157 får barn under tolv år till och med undantas från kravet på "säkerhetsdetaljen" fingeravtryck och barn under sex år undantas helt från detta krav enligt artikel 3.7 i förordning (EU) 2019/1157. Långt viktigare är emellertid att personer för vilka upptagning av fingeravtryck är fysiskt omöjlig ska undantas från kravet att lämna fingeravtryck. Vad som då över huvud taget är poängen med denna säkerhetsdetalj anges inte i förordning (EU) 2019/1157 och frågan lämnas helt enkelt obesvarad.
- 40 Den Europeiska datatillsynsmannen betonar dessutom i sitt yttrande att artikel 35.10 är tillämplig på åtgärder för upptagande och behandling av fingeravtryck. Enligt artikel 35.1 i den allmänna dataskyddsförordningen ska en konsekvensbedömning avseende dataskydd genomföras innan en behandling sker som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Konsekvensbedömningen avseende dataskydd ska i synnerhet omfatta en bedömning av riskerna för de registrerades rättigheter och friheter samt åtgärder för att hantera riskerna, inbegripet skyddsåtgärder och säkerhetsåtgärder.
- 41 Eftersom [behandlingen] har en rättslig grund i unionsrätten som den personuppgiftsansvarige omfattas av och den rätten reglerar den aktuella specifika behandlingsåtgärden, ska en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund genomföras (artikel 35.10 i den allmänna dataskyddsförordningen). En sådan konsekvensbedömning borde följaktligen ha

genomförts när förordning (EU) 2019/1157 antogs. Det framgår av skälen i förordningen att så inte skett.

- 42 Den hänskjutande domstolen stödjer den ståndpunkt som den Europeiska datatillsynsmannen uttrycker i sitt yttrande, nämligen att obligatoriskt införande av både ansiktsbilder och (två) fingeravtryck i identitetskort inte skulle ha godtagits inom ramen för en konsekvensbedömning. Redan under lagstiftningsförfarandet rekommenderade den Europeiska datatillsynsmannen därför att en ny bedömning görs av huruvida behandling av biometriska uppgifter (ansiktsbild i kombination med fingeravtryck) är nödvändigt och proportionerligt i detta sammanhang.
- 43 Lagstiftaren berör endast denna problematik vad gäller den allmänna dataskyddsförordningen i mycket allmänna ordalag i skäl 40 i förordningen. Den innehåller endast vaga uttryck som att medborgarna bör informeras om lagringsmediet och att det är nödvändigt att fastställa ytterligare skyddsåtgärder för behandlingen av personuppgifter, i synnerhet känsliga uppgifter såsom biometriska kännetecken. Lagringsmediet bör vidare vara mycket säkert och effektivt skydda de personuppgifter som lagras på det mot obehörig åtkomst. Det förblir oklart vad som menas med ”mycket säkert” och hur skyddsåtgärder och säkerhetsåtgärder ska vara utformade. I synnerhet förekommer ingen avvägning avseende riskerna vid en dataläcka från chipet och intrånget i artiklarna 7 och 8 i stadgan.
- 44 Därför uppkommer frågan huruvida en underlåtelse att genomföra en konsekvensbedömning avseende risker inte påverkar en bestämmelses verkan, eller om det tvärtom, när det föreligger en tvingande skyldighet för lagstiftaren att genomföra en konsekvensbedömning avseende risker, innebär att bestämmelsen är ogiltig om en sådan inte genomförts. I annat fall skulle lagstiftaren belönas för sin lagöverträdelse.