Yttrande 11/2024 om användningen av ansiktsigenkänning för att effektivisera passagerarflödet på flygplatser (förenlighet med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen)

Version 1.1

Antaget den 23 maj 2024

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

Version 1.1	den 28 maj 2024	Grammatisk rättelse i sammanfattningen (sidorna 3 och 4) och punkterna 77 och 90 i yttrandet
Version 1.0	den 23 maj 2024	Antagande av yttrandet

Sammanfattning

Den franska tillsynsmyndigheten begärde ett yttrande från Europeiska dataskyddsstyrelsen om användningen av ansiktsigenkänningsteknik för biometrisk autentisering eller identifiering av passagerare i syfte att effektivisera passagerarflödet på flygplatser. Tanken är att det är flygplatsers ledningsenheter och flygbolagen som ska använda sig av tekniken.

Först och främst påminner dataskyddsstyrelsen om att användningen av biometriska uppgifter, och i synnerhet ansiktsigenkänningsteknik, ökar riskerna för de registrerades rättigheter och friheter. I det här fallet är det biometriska uppgifter som ska behandlas och de är särskilt skyddade genom artikel 9 i dataskyddsförordningen. Denna teknik kan förvisso anses vara särskilt effektiv, men innan den används bör de personuppgiftsansvariga ändå bedöma konsekvenserna för de grundläggande rättigheterna och friheterna och överväga mindre inkräktande metoder för att uppnå det berättigade ändamålet med behandlingen.

Enligt begäran ska detta yttrande endast omfatta huruvida behandlingen är förenlig med **artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen** för det **särskilda syftet att effektivisera passagerarflödet på flygplatser** vid fyra specifika kontrollpunkter, närmare bestämt vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger. Yttrandet ger ingen fullständig eller utförlig analys av huruvida den eller de berörda personuppgiftsansvariga (eller i förekommande fall deras personuppgiftsbiträden) i varje enskilt fall efterlever dataskyddsförordningen. Det har därför ingen påverkan på rättsliga och tekniska analyser av de personuppgiftsansvarigas specifika planerade behandlingar och omständigheter i enskilda fall. De frågor som i begäran ställts till dataskyddsstyrelsen omfattar inte heller någon analys av den tillämpliga rättsliga grunden. Huruvida ett samtycke till sådan behandling är giltigt enligt artiklarna 6, 7 och 9 i dataskyddsförordningen prövas därför inte här. Yttrandet påverkar inte heller de begränsningar av användningen av biometriska uppgifter som föreskrivs i medlemsstaternas lagstiftning.

I detta yttrande bedömer dataskyddsstyrelsen behandlingens förenlighet med ovannämnda bestämmelser i dataskyddsförordningen inom ramen för **fyra specifika scenarier**.

I det **första scenariot** har enskilda personer själva kontroll över lagringen av en registrerad biometrisk mall som ska användas till att autentisera dem (genom en-till-en-verifiering) vid de ovannämnda flygplatskontrollpunkterna. Mallen kan till exempel lagras på den egna enheten.

Dataskyddsstyrelsen drar slutsatsen att de valda åtgärderna kan anses uppfylla nödvändighetsprincipen om den personuppgiftsansvarige kan visa att det inte finns några alternativa lösningar som är mindre inkräktande och kan uppnå samma mål lika effektivt. Dessutom kan behandlingens intrång uppvägas av att passagerarna aktivt deltar i behandlingen eftersom de själva har kontroll över lagringen av deras biometriska mall. Mallen kan till exempel lagras på passagerarens egen enhet. Deras uppgifter raderas också kort efter det att matchningen har genomförts. Dataskyddsstyrelsen drar därför slutsatsen att behandlingen i det första scenariot **i princip kan anses vara förenlig med artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen**, förutsatt att lämpliga skyddsåtgärder genomförs.

Dataskyddsstyrelsen har angett vilka skyddsåtgärder som åtminstone bör genomföras vid en lösning som liknar det första scenariot.

I det **andra scenariot** lagras en registrerad biometrisk mall centralt, på flygplatsen, i krypterad form och med en nyckel eller ett lösenord som endast passageraren själv har tillgång till. På så vis kan passagerare autentiseras (genom en-till-en-verifiering) när de passerar ovannämnda kontrollpunkter på flygplatsen. Den registrerade mallen är giltig en viss period, som till exempel kan vara upp till ett år efter deras senaste flygresa och fram till passets sista giltighetsdag.

Dataskyddsstyrelsen drar slutsatsen att behandlingen kan anses uppfylla nödvändighetsprincipen om den personuppgiftsansvarige kan visa att det inte finns några alternativa lösningar som är mindre inkräktande och kan uppnå samma mål lika effektivt. Dessutom kan behandlingens intrång uppvägas av att passagerarna aktivt deltar i behandlingen eftersom det enbart är de själva som har kontroll över nyckeln eller lösenordet till deras krypterade biometriska uppgifter. Om man utgår från att den personuppgiftsansvarige vidtar lämpliga skyddsåtgärder kan säkerhetsriskerna med att använda en central databas i detta scenario minimeras, och de negativa konsekvenserna för de registrerades grundläggande rättigheter och friheter kan anses stå i proportion till den förväntade nyttan. När det gäller principen om lagringsminimering har dataskyddsstyrelsen inte fått någon information som kan berättiga den långa lagringsperioden. Om detta scenario ska vara förenligt med artikel 5.1 e i dataskyddsförordningen bör de personuppgiftsansvariga kunna motivera varför den planerade lagringsperioden är nödvändig för ändamålet i specifika fall. Dataskyddsstyrelsen rekommenderar de personuppgiftsansvariga att välja kortast möjliga lagringsperiod och även ge passagerarna möjlighet att själva ange vilken lagringsperiod de föredrar. På dessa grunder drar dataskyddsstyrelsen slutsatsen att den behandling som planeras i scenario 2 **i princip kan anses vara förenlig med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen**, förutsatt att lämpliga skyddsåtgärder genomförs.

Dataskyddsstyrelsen har angett vilka skyddsåtgärder som åtminstone bör genomföras vid en lösning som liknar det andra scenariot.

I det **tredje scenariot** lagras en registrerad biometrisk mall centralt, i krypterad form, på flygplatsen och det är flygplatsens ledningsenhet som kontrollerar den. På så vis kan passagerare identifieras (genom en-till-N-verifiering) när de passerar ovannämnda kontrollpunkter på flygplatsen. Lagringsperioden i detta scenario är vanligtvis 48 timmar och uppgifterna raderas när planet har startat.

Eftersom identifieringsuppgifterna och de biometriska uppgifterna lagras i en central databas finns det en risk att åtkomst ges till hela uppsättningen uppgifter och till att obehörig eller olaglig identifiering görs av passagerarna i andra miljöer om databasens konfidentialitet bryts. Lagringsstrukturen är centraliserad och kontrolleras av flygplatsens ledningsenhet, vilket även innebär att passagerarna i högre grad förlorar kontrollen över sina uppgifter. Dataskyddsstyrelsen anser att det går att uppnå ett mer eller mindre lika effektivt passagerarflöde på flygplatser på ett mindre inkräktande sätt, och att de negativa konsekvenserna för de registrerades grundläggande rättigheter och friheter vid en eventuell uppgiftsincident i en central databas med biometriska uppgifter kan bli större än den förväntade nyttan av behandlingen. En sådan behandling kan alltså inte uppfylla nödvändighets- och proportionalitetsprinciperna. Dataskyddsstyrelsen drar därför slutsatsen att den behandling som avses i det tredje scenariot **inte kan vara förenlig med artikel 25 i dataskyddsförordningen**. Den **skulle inte heller vara förenlig med artikel 5.1 f eller artikel 32 i dataskyddsförordningen** om den personuppgiftsansvarige enbart vidtar de åtgärder som beskrivs i detta scenario.

I det **fjärde scenariot** lagras en registrerad biometrisk mall centralt i krypterad form i molnet, och det är flygbolaget eller dess molntjänstleverantör som har kontroll över den. På så vis kan passagerare

identifieras (genom en-till-N-verifiering) när de passerar ovannämnda kontrollpunkter på flygplatsen. I detta scenario skulle uppgifterna kunna lagras så länge som kunden har ett konto hos flygbolaget.

Eftersom identifieringsuppgifterna och de biometriska uppgifterna lagras i en central databas i molnet skulle flera enheter kunna få tillgång till dem, eventuellt även leverantörer utanför EES. Passagerarens uppgifter dekrypteras när de används och nycklarna kontrolleras av flygbolaget eller dess personuppgiftsbiträden, vilket innebär att angreppsytan kan bli större. Den centraliserade lagringsstrukturen innebär också att passagerarna i högre grad förlorar kontrollen över sina uppgifter. Uppgifterna kan också lagras under en lång tidsperiod, vilket ökar riskerna för en säkerhetsincident och inte tycks vara absolut nödvändigt och proportionerligt för behandlingens ändamål såvida inte fler tydliga åtgärder vidtas för att minimera riskerna för enskilda personer.

Dataskyddsstyrelsen anser att det går att uppnå ett mer eller mindre lika effektivt passagerarflöde på flygplatser på ett mindre inkräktande sätt och att de negativa konsekvenserna för de registrerades grundläggande rättigheter och friheter vid en eventuell uppgiftsincident i en central databas med biometriska uppgifter verkar vara större än den förväntade nyttan av behandlingen. En sådan behandling kan alltså inte uppfylla nödvändighets- och proportionalitetsprinciperna. Dataskyddsstyrelsen drar därför slutsatsen att den behandling som avses i det fjärde scenariot **inte kan vara förenlig med artikel 25 i dataskyddsförordningen**. Den **är inte heller förenlig med artikel 5.1 e i dataskyddsförordningen** utifrån den information som dataskyddsstyrelsen har tillgång till och **skulle inte vara förenlig med artikel 5.1 f eller artikel 32 i dataskyddsförordningen** om den personuppgiftsansvarige enbart vidtar de åtgärder som beskrivs i detta scenario.

Innehållsförteckning

Europeiska dataskyddsstyrelsen har antagit följande yttrande

med beaktande av artiklarna 63 och 64.2 i 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 (nedan kallad **dataskyddsförordningen**),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 10 och 22 i Europeiska dataskyddsstyrelsens (nedan kallad **dataskyddsstyrelsen**) arbetsordning, och

av följande skäl:

(1) Dataskyddsstyrelsens huvuduppgift är att säkerställa att dataskyddsförordningen tillämpas på ett och samma sätt i hela Europeiska ekonomiska samarbetsområdet (nedan kallat **EES**). Enligt artikel 64.2 i dataskyddsförordningen får varje tillsynsmyndighet, dataskyddsstyrelsens ordförande eller kommissionen i syfte att erhålla ett yttrande begära att styrelsen granskar en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat i EES.

(2) Dataskyddsstyrelsens yttrande ska antas i enlighet med artikel 64.3 i dataskyddsförordningen, jämförd med artikel 10.2 i dataskyddsstyrelsens arbetsordning, inom åtta veckor efter att ordföranden och behörig tillsynsmyndighet har beslutat att ärendets akt är fullständig. Ordföranden får besluta att förlänga denna period med ytterligare sex veckor med hänsyn till sakfrågans komplexitet.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

1 INLEDNING

1.1 Sammanfattning av sakförhållandena

1. Den 16 februari 2024 begärde den franska tillsynsmyndigheten att dataskyddsstyrelsen skulle avge ett yttrande om huruvida flygplatsernas ledningsenheters och flygbolagens användning av ansiktsigenkänningsteknik för biometrisk autentisering eller identifiering av passagerare[2], i syfte att effektivisera passagerarflödet vid flygplatsernas säkerhetskontroller[3], bagageinlämning, ombordstigning och tillträde till passagerarlounger (med undantag för gränskontroller och kontroller som utförs av skattefria butiker), är förenlig med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen (nedan kallad **begäran**). Den franska tillsynsmyndigheten bifogade en beskrivning av typiska användningsfall (bilaga I) till begäran.

[1] Hänvisningar till **medlemsstater** i detta yttrande bör förstås som hänvisningar till medlemsstater i EES. Hänvisningar till unionen eller EU i detta yttrande bör förstås som hänvisningar till EES.
[2] I detta yttrande avses med **passagerare** en registrerad person vars personuppgifter behandlas för det specifika ändamål som beskrivs i detta yttrande. Begreppen ”passagerare” och ”(enskild) person” används omväxlande och avser samma sak i resten av texten.
[3] I detta yttrande avses med **flygplatsernas säkerhetskontroller** de säkerhetskontroller som utförs under flygplatsens ledningsenhets ansvar och som passagerarna måste gå igenom från avgångshallen för att komma till gateområdet.

2. I begäran konstaterar den franska tillsynsmyndigheten att de modeller som för närvarande testas på flera flygplatser i EU skiljer sig åt mellan medlemsstaterna, vilket riskerar att leda till skillnader mellan tillsynsmyndigheternas tolkningar och att de registrerades grundläggande rättigheter och friheter i EU påverkas på olika sätt[4].

3. Dataskyddsstyrelsen anser att följande frågor måste besvaras för att kunna svara på denna begäran:

4. **Fråga 1:**

1.1. Kan användningen av ansiktsigenkänningsteknik för biometrisk autentisering **i det specifika syftet att effektivisera passagerarflödet på flygplatser** (vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger) vara förenlig med **artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen** om det gäller en lagringsstruktur där **enskilda personer själva** lagrar sin biometriska mall, till exempel lokalt på den egna enheten, och ingen annan har kontroll över den?

1.2. Om en sådan behandling konstateras vara förenlig med ovannämnda bestämmelser, vilka lämpliga minimiskyddsåtgärder skulle behövas mot bakgrund av artiklarna 25 och 32 i dataskyddsförordningen?

Fråga 2:

2.1. Kan användningen av ansiktsigenkänningsteknik för biometrisk autentisering eller identifiering **i det specifika syftet att effektivisera passagerarflödet på flygplatser** (vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger) vara förenlig med **artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen** om det gäller en **centraliserad** lagringsstruktur, där varje passagerares biometriska mall lagras i en central databas enligt följande:

2.1.1 I en central databas på flygplatsen som flygplatsens ledningsenhet kontrollerar, i krypterad form och med en nyckel eller ett lösenord som endast den enskilde själv har tillgång till (till exempel i dennes mobiltelefon), i autentiseringssyfte?

2.1.2 Om en sådan behandling konstateras vara förenlig, vilka lämpliga minimiskyddsåtgärder skulle behövas mot bakgrund av artiklarna 25 och 32 i dataskyddsförordningen?

2.2.1 I en central databas, på flygplatsen, som flygplatsens ledningsenhet kontrollerar, i krypterad form och med nycklar som innehas av samma ledningsenhet, i identifieringssyfte?

2.2.2 Om en sådan behandling konstateras vara förenlig, vilka lämpliga minimiskyddsåtgärder skulle behövas mot bakgrund av artiklarna 25 och 32 i dataskyddsförordningen?

[4] Begäran, s. 1.

2.3.1 I molnet, under flygbolagets eller dess tjänsteleverantörs (personuppgiftsbiträdes) kontroll, i krypterad form och med nycklar som innehas av flygbolaget eller dess tjänsteleverantör, i identifieringssyfte?

2.3.2 Om en sådan behandling konstateras vara förenlig, vilka lämpliga minimiskyddsåtgärder skulle behövas mot bakgrund av artiklarna 25 och 32 i dataskyddsförordningen?

5. Den franska tillsynsmyndigheten ansåg att ärendeakten var färdigställd den 16 februari 2024 och styrelsens ordförande ansåg att ärendeakten var färdigställd den 23 februari 2024. Efter det skickades ärendet ut av sekretariatet den 23 februari 2024. Styrelsens ordförande beslutade, i enlighet med artikel 64.3 i dataskyddsförordningen jämförd med artikel 10.2 i dataskyddsstyrelsens arbetsordning, att förlänga standardtidsfristen på åtta veckor med ytterligare sex veckor på grund av sakfrågans komplexitet.

1.2 Tillåtligheten av begäran om ett yttrande enligt artikel 64.2 i dataskyddsförordningen

6. Enligt artikel 64.2 i dataskyddsförordningen får varje tillsynsmyndighet, i syfte att erhålla ett yttrande, begära att dataskyddsstyrelsen granskar en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat.

7. Dataskyddsstyrelsen anser att den begäran som den franska tillsynsmyndigheten hänvisar till om förenligheten hos användningen av ansiktsigenkänningsteknik för biometrisk autentisering eller identifiering i det specifika syftet att effektivisera passagerarflödet på flygplatser avser frågor som ”har följder i mer än en medlemsstat”. Som man skriver i begäran[5] är nämligen flera olika projekt på gång just nu på medlemsstaternas flygplatser, och antagligen kommer sådan användning att öka under de kommande åren. De modeller som olika flygplatser och flygbolag för närvarande testar skiljer sig avsevärt åt mellan medlemsstaterna, och ur dataskyddssynpunkt kan detta medföra en risk för att det får olika följder i mer än en medlemsstat.

8. Dataskyddsstyrelsen anser också att den begäran som den franska tillsynsmyndigheten hänvisar till har betydande konsekvenser för tillämpningen av de principer som fastställs i artikel 5.1 e och f i dataskyddsförordningen, de krav som gäller för personuppgiftsansvariga enligt artikel 25 i dataskyddsförordningen samt de krav som gäller för personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 32 i dataskyddsförordningen. Denna begäran avser därför en ”fråga med allmän räckvidd” i den mening som avses i artikel 64.2 i dataskyddsförordningen, eftersom den rör en enhetlig tolkning av principerna om lagringsminimering (artikel 5.1 e i dataskyddsförordningen) och om integritet och konfidentialitet (artikel 5.1 f i dataskyddsförordningen), och begreppen inbyggt dataskydd och dataskydd som standard (artikel 25 i dataskyddsförordningen) och datasäkerhet (artikel 32 i dataskyddsförordningen) i syfte att säkerställa, bland annat, att dessa bestämmelser tillämpas på ett och samma sätt i hela EES.

9. Om medlemsstaternas tolkningar av artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen skiljer sig åt kan risken öka för att flygplatsers ledningsenheter och flygbolag utvecklar projekt för ansiktsigenkänning som inte är enhetliga. Den franska tillsynsmyndigheten har visat att det finns ett tydligt behov av en enhetlig tolkning av dessa bestämmelser när det gäller ansiktsigenkänningsteknik för biometrisk autentisering eller identifiering av passagerare i syfte att

[5] Begäran, s. 3.

effektivisera passagerarflödet på flygplatser[6], och dataskyddsstyrelsen anser därför att begäran är motiverad i enlighet med artikel 10.3 i dataskyddsstyrelsens arbetsordning.

10. Enligt artikel 64.3 i dataskyddsförordningen ska dataskyddsstyrelsen inte avge ett yttrande om den redan har avgett ett yttrande i frågan[7]. Dataskyddsstyrelsen har ännu inte lämnat några svar på de frågor som följer av begäran. Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter[8] innehåller visserligen några användbara delar om vilka säkerhetsåtgärder som bör vidtas när biometriska uppgifter behandlas, men de avhandlar inte alla aspekter av frågorna i begäran. Den vägledning som dataskyddsstyrelsen tillgängliggjort – däribland dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter – innehåller inte heller någon särskild vägledning om vilka eventuella faktorer som ska kontrolleras i samband med att biometriska uppgifter lagras, centraliserat eller decentraliserat, för identifiering eller autentisering av passagerare i syfte att effektivisera passagerarflödet på flygplatser, och inte heller något om en sådan behandlings förenlighet med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen.

11. Av dessa skäl anser dataskyddsstyrelsen att begäran är tillåtlig och att frågorna som lyfts däri bör analyseras i ett yttrande som ska antas i enlighet med artikel 64.2 i dataskyddsförordningen.

2 YTTRANDETS OMFATTNING OCH BAKGRUND

2.1 Yttrandets omfattning

12. Detta yttrande rör endast frågan om huruvida flygplatsernas ledningsenheters och flygbolagens användning av ansiktsigenkänningsteknik för biometrisk autentisering eller identifiering av passagerare **i det specifika syftet att effektivisera passagerarflödet på flygplatser**, närmare bestämt vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger, är förenlig med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen, i enlighet med vad som anges i begäran.

13. När det gäller **yttrandets omfattning** klargör dataskyddsstyrelsen följande:

    1) Behandling av personuppgifter inom ramen för gränskontroller eller kontroller som utförs av skattefria butiker omfattas inte av detta yttrande, eftersom de utförs av andra personuppgiftsansvariga än de vid flygplatsernas ledningsenheter eller vid flygbolagen.

    2) Användningen av ansiktsigenkänningsteknik för andra ändamål (såsom brottsbekämpning) eller av andra parter faller utanför detta yttrandes omfattning, även om den grundar sig på de scenarier som beskrivs nedan i avsnitt 3.2 eller har likartade ändamål.

    3) Detta yttrande granskar endast behandlingen av passagerares personuppgifter och omfattar inte andra typer av registrerade personer, såsom personal vid flygplatsernas ledningsenheter eller vid flygbolagen.

[6] Begäran, s. 1–3.
[7] Artikel 64.3 i dataskyddsförordningen och artikel 10.4 i dataskyddsstyrelsens arbetsordning.
[8] Dataskyddsstyrelsens riktlinjer 3/2019 för behandling av personuppgifter genom videoenheter, version 2.0, antagna den 29 januari 2020 (nedan kallade **dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter**).

4) I detta yttrande granskas den begäran som lämnats in av den franska tillsynsmyndigheten med avseende på huruvida lagringsstrukturerna för passagerarnas biometriska mallar är förenliga med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen. Det innehåller i detta avseende ingen fullständig eller utförlig analys av huruvida den eller de berörda personuppgiftsansvariga (eller deras personuppgiftsbiträden, i förekommande fall) efterlever dataskyddsförordningen i varje enskilt fall. Detta är särskilt viktigt eftersom sådan teknik medför ökade risker i samband med behandlingen av de särskilda uppgiftskategorierna enligt artikel 9 i dataskyddsförordningen. Yttrandet påverkar därför inte bedömningar av andra bestämmelser i dataskyddsförordningen när det gäller användningen av teknik för ansiktsigenkänning, inte heller inom den specifika sektor som begäran gäller, eller rättsliga och tekniska analyser som avser personuppgiftsansvarigas specifika planerade behandlingar och omständigheter i enskilda fall.

5) Detta yttrande rör inte behandlingen av barns personuppgifter och har ingen påverkan på eventuella särskilda krav som gäller i sådana frågor.

6) Detta yttrande har ingen påverkan på rättsliga krav eller andra begränsningar av användningen av biometriska uppgifter som härrör från medlemsstaternas nationella lagstiftning[9].

7) Eventuella slutsatser i detta yttrande påverkar inte den fortsatta tekniska utvecklingen.

8) I detta yttrande undersöks fyra scenarier, vars särdrag beskrivs nedan i avsnitt 3.2. Det tar inte upp andra scenarier, även om behandlingen skulle ha samma ändamål.

14. I begäran angav den franska tillsynsmyndigheten att behandlingen av passagerarnas biometriska uppgifter i syfte att effektivisera passagerarflödet på flygplatser skulle göras på grundval av antagandet att passagerarna samtycker till sådan behandling, vilket eventuellt skulle utgöra den rättsliga grunden enligt dataskyddsförordningen[10]. **Analysen av den tillämpliga rättsliga grunden omfattas dock inte av de frågor som ställts till dataskyddsstyrelsen i begäran och huruvida samtycke till sådan behandling är giltigt i enlighet med artiklarna 6, 7 och 9 i dataskyddsförordningen behandlas därför inte i detta yttrande.**

15. Dataskyddsstyrelsen noterar dock i allmänna ordalag att om de berörda personuppgiftsansvariga skulle förlita sig på denna rättsliga grund skulle de ändå behöva inhämta ett giltigt uttryckligt samtycke[11] från varje enskild person som är villig att använda sådana tjänster. Ett sådant uttryckligt

[9] I artikel 9.4 i dataskyddsförordningen föreskrivs till exempel att medlemsstaterna får behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av biometriska uppgifter.
[10] Begäran, bilaga I.
[11] Enligt artiklarna 4.14, 9.1 och 9.2 a i dataskyddsförordningen ska behandling av biometriska uppgifter i syfte att entydigt identifiera en fysisk person vara förbjuden, såvida inte den registrerade uttryckligen har gett sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i artikel 9.1 i dataskyddsförordningen inte kan upphävas av den registrerade. Se även skälen 51, 52 och 53 i dataskyddsförordningen.

samtycke måste vara frivilligt, specifikt och informerat[12], och huruvida dessa villkor är uppfyllda skulle behöva analyseras i varje enskilt fall. Detta innebär bland annat följande:

1) Enskilda personer måste enkelt kunna dra tillbaka ett sådant samtycke när som helst och utan att problem uppstår[13].

2) Om samtycket ska kunna lämnas frivilligt kan sådan användning av biometrisk teknik endast ske på frivillig basis, eftersom enskilda personer bör kunna välja fritt om de vill använda dessa tjänster eller inte, utan att det leder till några problem (såsom betydligt längre väntetider för passagerare som inte samtycker[14]) eller extra kostnader och utan incitament eller extra fördelar i utbyte[15].

3) Uttryckligt samtycke skulle också behöva inhämtas från enskilda personer vars biometriska uppgifter behandlas trots att de inte har registrerat sig i syfte att identifieras eller autentiseras på detta sätt. Med andra ord är det oerhört viktigt att enskilda personer som inte uttryckligen har samtyckt till ansiktsigenkänning för det avsedda ändamålet inte får sina ansikten skannade med kameror. Detta kan till exempel uppnås genom att man skapar särskilda köer för ansiktsigenkänning och sätter upp tydliga skyltar och rent fysiskt separerar dem från de kontroller som inte använder biometri så att det blir lätt att urskilja vilken kö som avser vad.

4) Principerna för behandling i artikel 5 i dataskyddsförordningen som avser nödvändighet och proportionalitet är tillämpliga även i de fall där personerna har lämnat sitt uttryckliga samtycke till att deras biometriska uppgifter används[16], utan att det påverkar frågan huruvida samtycke skulle vara den tillämpliga rättsliga grunden för sådan behandling.

16. I begäran anges[17] det att flygplatsernas ledningsenheter skulle agera som personuppgiftsansvariga när det gäller behandlingen vid flygplatsernas säkerhetskontroller, medan flygbolagen skulle agera som personuppgiftsansvariga när det gäller behandlingen vid bagageinlämning, ombordstigning och tillträde till passagerarlounger. Dataskyddsstyrelsen konstaterar därför att flera olika aktörer kan vara inblandade i de behandlingar som beskrivs i begäran och den har inte bedömt hur rollerna som (gemensamt ansvariga) personuppgiftsansvariga och/eller personuppgiftsbiträden ska tillämpas i de scenarier som beskrivs nedan i avsnitt 3.2 i detta yttrande. I varje enskilt fall måste det gå att identifiera de berörda aktörerna och deras ansvarsområden måste vara tydligt fördelade om kraven i dataskyddsförordningen ska kunna uppfyllas[18].

---

[12] Artiklarna 4.11 och 7 i dataskyddsförordningen.
[13] Artikel 7.4 i dataskyddsförordningen samt skäl 50 i dataskyddsförordningen.
[14] Det kan till exempel omfatta överväganden om att utforma ett system som inte skapar ett socialt tryck på passagerare som inte vill ge sitt samtycke genom att se till att valet inte påverkar andra passagerare negativt.
[15] Dataskyddsstyrelsens riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, version 1.1, antagna den 4 maj 2020 (nedan kallade **dataskyddsstyrelsens riktlinjer 5/2020 om samtycke**), punkterna 46 och 48.
[16] Ibid., punkt 5.
[17] Begäran, bilaga I.
[18] I linje med artiklarna 4.7, 4.8, 5.2, 24, 26, 28 och 29 i dataskyddsförordningen. Se även dataskyddsstyrelsens riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.1, antagna den 7 juli 2021.

17. Dataskyddsstyrelsen konstaterar också att det för närvarande inte finns något enhetligt rättsligt krav i EU på flygplatsernas ledningsenheter eller flygbolagen att identifiera passagerare eller att kontrollera att namnet på passagerarens boardingkort överensstämmer med namnet på deras identitetshandling vid alla ovannämnda kontrollpunkter[19]. Det är den nationella lagstiftningen som anger sådana krav och den kan skilja sig åt medlemsstaterna emellan. I några medlemsstater kan sådana kontroller krävas vid vissa kontrollpunkter (t.ex. vid bagageinlämning eller ombordstigning), medan det i andra inte krävs några sådana kontroller alls i dag[20]. De rättsliga skyldigheterna att kontrollera passagerarnas identitet har en direkt inverkan på de olika flygplatsernas praxis.

18. I situationer **där passagerarnas identitet inte måste verifieras med en officiell identitetshandling bör följaktligen ingen verifiering göras med hjälp av biometriska uppgifter. Detta skulle leda till en överdriven behandling av uppgifter eftersom fler uppgifter då behandlas jämfört med den nuvarande situationen, och det skulle gå utöver vad som är nödvändigt för det relevanta ändamålet och därmed strida mot principen om uppgiftsminimering enligt artikel 5.1 c i dataskyddsförordningen**. Detta ska has i åtanke vid granskningen av samtliga scenarier som beskrivs i avsnitt 3.2 i detta yttrande.

2.2 Nyckelbegrepp

19. För att klassificeras som biometriska uppgifter enligt artikel 4.14 i dataskyddsförordningen[21] bör behandlingen av rådata, såsom en fysisk persons fysiska, fysiologiska eller beteendemässiga egenskaper, innebära en mätning av dessa egenskaper, eftersom biometriska uppgifter är resultatet av sådana mätningar[22].

20. Med hjälp av en bild av en persons ansikte (ett fotografi eller videoklipp), vilket kallas ett biometriskt **prov**, kan man ta fram en digital återgivning av ansiktets unika kännetecken (en så kallad **mall**)[23]. Dataskyddsstyrelsen påminner också om att ”[e]n biometrisk mall är en digital återgivning av de unika kännetecken som har hämtats från ett biometriskt prov och kan lagras i en biometrisk databas”[24] som möjliggör eller bekräftar identifieringen av en fysisk person. ”Denna mall förväntas [dessutom] vara unik och specifik för varje person, och är i princip permanent över tid”[25]. I en jämförelseprocess som syftar till att identifiera eller autentisera en person genom ansiktsigenkänning jämförs vanligtvis en

[19] Den relevanta förordningen på EU-nivå är kommissionens genomförandeförordning (EU) 2015/1998 av den 5 november 2015 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd. Denna förordning omfattar dock inte kontroller av officiella identitetshandlingar vid kontrollpunkter på flygplatser, och medlemsstaterna har rätt att själva reglera detta på nationell nivå.

[20] Det betyder att det för närvarande antingen inte görs någon kontroll alls eller att man endast kontrollerar att personen har ett boardingkort. Till exempel är medborgare i Norge, Danmark, Finland och Sverige från och med den 1 juli 1954 undantagna från skyldigheten att inneha pass eller annan reseidentifiering när de reser mellan dessa länder, på grundval av Protokollet angående befrielse för nordiska medborgare från att under uppehåll i annat nordiskt land än hemlandet innehava pass och uppehållstillstånd av den 22 maj 1954.

[21] Se även skälen 51, 52 och 53 i dataskyddsförordningen.

[22] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 74.

[23] Dataskyddsstyrelsens riktlinjer 05/2022 om användningen av teknik för ansiktsigenkänning på brottsbekämpningsområdet, version 2.0, antagna den 26 april 2023 (nedan kallade **dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning**), punkterna 7 och 8.

[24] Ibid., punkt 9.

[25] Ibid.

inkommande biometrisk mall mot redan lagrade objekt i syfte att antingen verifiera en matchning eller hitta en matchning i en databas[26].

21. Ansiktsigenkänningsteknik kan fylla två olika funktioner – autentisering[27] och identifiering[28]. Funktionerna skiljer sig åt, men båda kräver att biometriska uppgifter som rör en identifierad eller identifierbar fysisk person behandlas[29] och utgör därför behandling av särskilda kategorier av personuppgifter enligt artikel 9 i dataskyddsförordningen[30].

22. Det rör sig framför allt om följande:

> **Autentisering** går ut på att bekräfta ett biometriskt påstående genom jämförelse. Detta kallas även en-till-en-verifiering.
>
> **Identifiering** går ut på att söka i en databas med registrerade biometriska mallar efter kännetecken som kan hänföras till en enskild person. Detta kallas även en-till-många-identifiering.

23. I båda fallen (dvs. identifiering och autentisering) baseras tekniken för ansiktsigenkänning på en uppskattad matchning mellan mallar, det vill säga den som ska jämföras och en eller flera referensmallar. I detta hänseende är tekniken probabilistisk, vilket innebär att jämförelsen leder till en högre eller lägre sannolikhet för att personen verkligen är den person som ska autentiseras eller identifieras. Om sannolikheten överstiger ett visst tröskelvärde i systemet, som fastställts av användaren eller systemutvecklaren, kommer systemet att anta att det har hittat en matchning som ska identifieras eller autentiseras[31].

---

[26] Dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning, punkterna 10–11; se även den internationella standarden ISO/IEC 2382–37, 2022–03,
som finns på: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [hämtad den 23 maj 2024] (nedan kallad **ISO/IEC 2382-37**).

[27] Dataskyddsstyrelsen konstaterar att Europaparlamentets och rådets kommande förordning om harmoniserade regler för artificiell intelligens (rättsakten om artificiell intelligens) (ännu ej offentliggjord i EUT) i artikel 3.36 även definierar *biometrisk verifiering* som ”automatiserad en-till-en-verifiering, inklusive autentisering, av fysiska personers identitet genom jämförelse av deras biometriska uppgifter med tidigare lämnade biometriska uppgifter” (se Europaparlamentets lagstiftningsresolution av den 13 mars 2024 om förslaget till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (COM(2021) 0206 – C9–0146/2021–2021/0106 (COD)).

[28] Ibid; i artikel 3.35 i rättsakten om artificiell intelligens definieras *biometrisk identifiering* som ”automatiserad igenkänning av fysiska, fysiologiska, beteendemässiga eller psykologiska mänskliga drag för att fastställa en fysisk persons identitet genom jämförelse av personens biometriska uppgifter med biometriska uppgifter om enskilda personer som lagrats i en databas”.

[29] ISO/IEC 2382–37.

[30] Artikel 4.14 i dataskyddsförordningen och dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning, punkt 12.

[31] Dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning, punkt 11. Se även ISO/IEC 2382–37.

3 OM BEGÄRANS SAKFÖRHÅLLANDEN

3.1 Allmänna kommentarer

24. I detta avsnitt analyseras de frågor som anges i punkt 4 ovan. Dataskyddsstyrelsen kommer för fråga 1 att analysera förenligheten med artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen, och för fråga 2 förenligheten med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen.

25. Den kommer därför att analysera fyra olika scenarier[32], vars särskilda egenskaper beskrivs nedan i avsnitt 3.2.

26. Först och främst påminner dataskyddsstyrelsen om att användningen av biometriska uppgifter, och i synnerhet ansiktsigenkänningsteknik, ökar riskerna för de registrerades rättigheter och friheter. Den aktuella behandlingen avser nämligen biometriska uppgifter som är särskilt skyddade enligt artikel 9 i dataskyddsförordningen. Framför allt ändrar biometriska uppgifter oåterkalleligt förhållandet mellan kropp och identitet, eftersom de gör att den mänskliga kroppens egenskaper blir ”maskinläsbara” och kan bli föremål för vidare användning[33]. Dessutom kan användningen av ansiktsigenkänningsteknik leda till risker i form av bland annat falska negativa resultat, systematiska fel (biaser) och diskriminering[34], och möjligheterna att missbruka biometriska uppgifter kan leda till allvarliga konsekvenser för enskilda personer, såsom identitetsbedrägeri eller identitetsmissbruk[35]. Det bör också noteras att när ansiktsigenkänning görs på distans och utan aktiv medverkan av den registrerade kan de enskilda personerna vara ännu mer omedvetna om sådan behandling och de risker som är förknippade med detta. Slutligen är det viktigt att betona att de egenskaper som de biometriska uppgifterna grundar sig på i allmänhet kan betraktas som permanenta och bör behandlas som oåterkalleliga. Detta gäller i synnerhet ansiktsigenkänning[36].

27. Med beaktande av ovanstående bör de personuppgiftsansvariga bedöma konsekvenserna för de grundläggande rättigheterna och friheterna innan denna teknik används, även om den kan anses vara särskilt effektiv, och överväga mindre inkräktande metoder för att uppnå det berättigade ändamålet med behandlingen[37].

---

[32] De fyra scenarier som har analyserats av dataskyddsstyrelsen bygger på de användningsfall som anges i bilaga I till begäran. Den franska tillsynsmyndigheten har klargjort att de användningsfall som anges i bilaga I till begäran är exempel på genomförande, att de hör till ett scenario och att de används i illustrativt syfte.

[33] Artikel 29-gruppens yttrande 3/2012 om utvecklingen i fråga om biometrisk teknik, antaget den 27 april 2012, WP193 (nedan kallat **artikel 29-gruppens yttrande 3/2012 om biometrisk teknik**), s. 4. Det bör noteras att detta yttrande hänvisar till direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (*dataskyddsdirektivet*). Dataskyddsförordningen har utvidgat tillämpningsområdet för de särskilda kategorierna av uppgifter, och till skillnad från dataskyddsdirektivet föreskriver dataskyddsförordningen att biometriska uppgifter är särskilda kategorier av uppgifter (artikel 9 i dataskyddsförordningen).

[34] *Guidelines on facial recognition* (inte översatt till svenska) från rådgivande kommittén för Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, juni 2021, s. 15, samt dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning, punkt 27.

[35] Artikel 29-arbetsgruppens yttrande 3/2012 om biometrisk teknik, s. 29.

[36] Dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning, punkt 104.

[37] Skäl 39 i dataskyddsförordningen. Se även dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 73.

28. Dataskyddsstyrelsen erinrar också om att rätten till skydd av personuppgifter inte är en absolut rättighet och att den bör vägas mot andra grundläggande rättigheter som är skyddade genom stadgan, i enlighet med proportionalitetsprincipen[38].

29. I artikel 25.1 i dataskyddsförordningen hänvisas till de ”dataskyddsprinciper” som förtecknas i artikel 5 i dataskyddsförordningen[39] och som kräver åtgärder som är utformade för ”ett effektivt genomförande”[40]. Detta gäller uttryckligen principen om uppgiftsminimering enligt artikel 5.1 c i dataskyddsförordningen[41], enligt vilken personuppgifter ska vara ”adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas”, med beaktande av proportionalitetsprincipen[42]. Dessutom anger artikel 25.2 i dataskyddsförordningen skyldigheten att minimera data som standard genom att ange att denna skyldighet gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet[43].

30. Artikel 25 i dataskyddsförordningen kräver dock inte att de personuppgiftsansvariga genomför några specifika tekniska och organisatoriska åtgärder, utan snarare att de åtgärder och skyddsåtgärder man väljer att vidta ska vara specifika för sammanhanget och de risker för den registrerades rättigheter och friheter som kan uppstå till följd av behandlingen[44]. På samma sätt anger artikel 32 i dataskyddsförordningen om säkerhet i samband med behandlingen att personuppgiftsansvariga och personuppgiftsbiträden ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för fysiska personers rättigheter och friheter.

31. Det är viktigt att notera att principerna om nödvändighet och proportionalitet i dataskyddsförordningen är tillämpliga även om passagerarna uttryckligen skulle samtycka till att deras

---

[38] Skäl 4 i dataskyddsförordningen. Se även domstolens dom av den 22 juni 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (nedan kallad *C-439/19 Latvijas Republikas Saeima*), punkterna 98, 110 och 113. Proportionalitetsprincipen, som är en allmän princip i unionsrätten, kräver dessutom att de medel som föreskrivs i en rättsakt från unionen är ägnade att säkerställa att det mål som eftersträvas uppnås och att de inte går utöver vad som är nödvändigt för att uppnå detta mål (se domstolens dom av den 9 november 2010, Volker und Markus Schecke och Eifert, C-92/09 och C-93/09, ECLI:EU:C:2010:662 [nedan kallad *C-92/09 och C-93/09 Volker und Schecke*], punkt 74 och där angiven rättspraxis).

[39] Dataskyddsstyrelsens riktlinjer 4/2019 om artikel 25 – Inbyggt dataskydd och dataskydd som standard, version 2.0, antagna den 20 oktober 2020 (nedan kallade **dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard**), punkt 11.

[40] I artikel 25.1 i dataskyddsförordningen föreskrivs följande: ”Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.” Se även dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 13.

[41] På motsvarande sätt anger skäl 39 i dataskyddsförordningen att personuppgifter endast bör behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel.

[42] C-439/19 Latvijas Republikas Saeima, punkt 98, och domstolens dom av den 11 december 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 (nedan kallad *C-708/18 M5A-ScaraA*), punkt 48.

[43] Dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 48.

[44] Dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 14.

biometriska uppgifter används för att effektivisera passagerarflödet på flygplatser, och dessa principer måste följas[45].

32. När det gäller **nödvändighetsprincipen** kommer dataskyddsstyrelsen att överväga om den föreslagna behandlingen är nödvändig för att uppnå det eftersträvade målet och om samma mål kan uppnås lika effektivt med andra medel som är mindre inkräktande när det gäller den registrerades grundläggande rättigheter och friheter[46]. När det gäller **proportionalitetsprincipen** kommer dataskyddsstyrelsen att bedöma huruvida de negativa konsekvenserna för de registrerades grundläggande rättigheter och friheter står i proportion till den eventuella förväntade nyttan. Om nyttan är relativt liten är en sådan påverkan kanske inte proportionerlig[47].

33. Dataskyddsstyrelsen kan mycket väl anse att något av de scenarier som analyseras nedan kan uppfylla kraven i artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen, men det åligger ändå den personuppgiftsansvarige att visa detta med faktiska omständigheter. I sådana fall bör även alternativa scenarier övervägas.

3.2 Om förenlighet med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen

3.2.1 Scenario 1: endast den enskilde personen har kontroll över lagringen av en registrerad biometrisk mall, i autentiseringssyfte

34. I detta avsnitt granskas hur förenligt det är med artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen att en biometriska mall i autentiseringssyfte lagras hos passageraren – till exempel på dennes egen enhet[48] – helt under dennas kontroll[49],[50] (nedan kallat **scenario 1**). I detta avsnitt undersöks också lämpliga skyddsåtgärder för scenario 1, mot bakgrund av artiklarna 25 och 32 i dataskyddsförordningen.

Beskrivning av scenariot

35. I scenario 1 lagras varje passagerares registrerade biometriska mall, om denne har samtyckt till sådan behandling, enbart hos passageraren själv, till exempel på dennes egen enhet. Passagerarna autentiseras (genom en-till-en-verifiering) när de går igenom särskilda kontrollpunkter på flygplatsen.

36. Registreringen görs av flygplatsens ledningsenhet, antingen på distans via dennes app[51] eller på flygplatsterminalen med lämplig säkerhetsnivå när det gäller identifieringen (t.ex. lämplig eIDAS-

[45] Dataskyddsstyrelsens riktlinjer 5/2020 om samtycke, punkt 5.
[46] C-439/19 Latvijas Republikas Saeima, punkterna 110 och 113, och domstolens dom (stora avdelningen) av den 4 juli 2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, punkt 108.
[47] C-708/18 M5A-ScaraA, punkterna 52–56, C-92/09 och C-93/09 Volker und Schecke, punkt 87, samt C-439/19 Latvijas Republikas Saeima, punkterna 98, 110 och 113. Se även artikel 29-arbetsgruppens yttrande 3/2012 om biometrisk teknik, s. 8.
[48] Som ett alternativ skulle personen kunna skriva ut och lagra sin biometriska mall på papper.
[49] Detta påverkar inte den personuppgiftsansvariges övergripande ansvar för behandlingen.
[50] Detta exemplifieras genom användningsfall 1 i bilaga I till begäran.
[51] Dataskyddsstyrelsen konstaterar att det i framtiden kan komma att gå att registrera sig på andra sätt och att registreringen kan gå att genomföra utan en specifik app från flygplatsens ledningsenhet, till exempel med hjälp av en användares digitala plånbok.

säkerhetsnivå[52]). Registreringen består i att en biometrisk mall och de identifieringsuppgifter[53] som är nödvändiga för behandlingen läggs in på passagerarens enhet. Registreringen sker endast en gång och är giltig under en viss tid (som kan vara lika lång som giltighetstiden för passagerarens pass). Efter själva registreringsprocessen lagrar flygplatsens ledningsenhet varken passagerarnas identifieringsuppgifter eller deras biometriska uppgifter.

37. Särskilt viktigt är att passagerarens identifieringsuppgifter och biometriska mall lagras lokalt på dennes egen enhet (t.ex. i flygplatsens ledningsenhets mobilapp eller i en digital plånboksapp). Enheten kan sedan användas för att överföra eller söka efter passagerarnas identifieringsuppgifter och biometriska mall, och kanske även flyginformation och/eller boardingkort. Exempelvis krypteras denna information med en nyckel som endast innehas av flygplatsens ledningsenhet – den kan kanske vara kodad i form av en QR-kod, som antingen kan skrivas ut på papper eller visas på skärmen på passagerarens enhet. I detta fall kan passageraren sedan visa fram QR-koden för särskilda kontrollenheter på flygplatsen som har en QR-skanner och en kamera.

38. När det gäller säkerhet dekrypteras QR-koderna vid matchningen med en nyckel som innehas av flygplatsens ledningsenhet, den ende som kan dekryptera QR-koderna. Passagerarnas biometriska uppgifter lagras endast under en mycket kort period och raderas när matchningen har genomförts. Det bör noteras att åtgärderna för en säker lagring delvis beror på hur säker passagerarens enhet är.

Dataskyddsstyrelsens bedömning

39. I scenario 1 beskrivs olika tekniska och organisatoriska åtgärder som är utformade för att säkerställa en lämplig säkerhetsnivå i förhållande till riskerna för de registrerade i enlighet med artiklarna 5.1 f och 32 i dataskyddsförordningen. Passagerarna autentiseras (genom en-till-en-verifiering) när de passerar särskilda kontrollpunkter på flygplatsen. I detta scenario sker den huvudsakliga matchningen i en kontrollerad miljö[54] där passagerarna själva aktivt deltar och har större kontroll över sina uppgifter. I synnerhet kontrolleras endast de passagerare som har samtyckt till sådan behandling, och eftersom kontrollen sker vid särskilt avsedda enheter kommer biometriska uppgifter om andra passagerare som inte har samtyckt till sådan behandling inte att samlas in. De passagerare som ger sitt samtycke har dessutom möjlighet att när som helst stoppa behandlingen genom att radera uppgifterna från sin enhet.

40. När ansiktsigenkänning sker med hjälp av en biometrisk mall som endast den enskilde personen själv kontrollerar, till exempel genom att den lagras på passagerarens egen enhet som bara denne har kontroll över, och som vid vissa kontrollpunkter används för autentisering genom ett särskilt gränssnitt kan riskerna under vissa omständigheter vara mindre än då man använder biometriska uppgifter som

[52] Ett ramverk för elektronisk identifiering och betrodda tjänster (nedan kallad **eIDAS**) på grundval av Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet.

[53] I detta yttrande avses med identifieringsuppgifter sådana uppgifter som med hjälp av en identitetshandling eller ett pass har befunnits korrekta, såsom efternamn, förnamn, födelsedatum osv.

[54] Okontrollerad miljö: användning av ansiktsigenkänning för identifiering utan aktiv medverkan av de registrerade, där mallen för varje ansikte i övervakningsområdet jämförs med mallar från ett brett tvärsnitt av befolkningen som lagras i en databas, se dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning, punkt 17.

lagras i en central databas[55]. Om sådan lagring åtföljs av lämpliga skyddsåtgärder[56] medför det att eventuella personuppgiftsincidenter blir mindre allvarliga jämfört med centraliserad lagring när det gäller antalet berörda personer. Det skulle också säkerställa att den registrerade aktivt medverkar i att ge tillgång till den biometriska mallen.

41. Matchningen kan dessutom göras lokalt på flygplatsen genom att den biometriska mallen, som till exempel kan avläsas i QR-koden, jämförs gentemot de utdata från mallen som beräknats fram utifrån det biometriska prov som tagits av kontrollenhetens kamera. Då är det bara matchningsresultatet som den personuppgiftsansvarige får ta del av och kan använda vid en särskild kontroll (det kan vara antingen flygplatsens ledningsenhet eller ett flygbolag beroende på om det görs vid flygplatsens säkerhetskontroller, bagageinlämning, ombordstigning och/eller tillträde till passagerarlounge). Att de uppgifter som krävs för matchningen (t.ex. QR-koden) måste tillhandahållas av de enskilda personerna själva fungerar också som en andra faktor[57], vilket stärker autentiseringens säkerhet.

42. När det gäller förenligheten med artikel 25 i dataskyddsförordningen, och i synnerhet för att uppfylla kravet på uppgiftsminimering, bör det säkerställas att behandlingen uppfyller nödvändighetsprincipen. I scenario 1 kan de valda åtgärderna anses ha uppfyllt nödvändighetsprincipen i förhållande till det eftersträvade ändamålet (dvs. att effektivisera passagerarflödet) om den personuppgiftsansvarige kan visa att det inte finns några alternativa lösningar som är mindre inkräktande och kan uppnå samma mål lika effektivt, beroende på omständigheterna kring behandlingen. Den personuppgiftsansvarige skulle till exempel kanske kunna visa att även om passageraren behöver visa fram sin enhet skulle scenario 1 påskynda kontrollprocessen jämfört med den nuvarande situationen, där en människa kontrollerar om namnet på boardingkortet stämmer överens med passagerarens identitetshandling[58]. Detta kan naturligtvis inte påvisas om det i dag inte görs några kontroller för att kontrollera passagerarnas identitet med hjälp av deras officiella identitetshandling (se i detta avseende punkt 18 ovan).

43. Vidare sparar flygplatsens ledningsenhet inte de biometriska mallarna efter registreringen och den personuppgiftsansvarige som utför kontrollen lagrar bara de biometriska uppgifterna under en mycket kort tid, eftersom de raderas så snart matchningen har slutförts. De valda åtgärderna i scenario 1 tycks således leda till att omfattningen av såväl behandlingen som lagringsperioden för personuppgifterna begränsas.

44. När det gäller proportionalitetsprincipen kan intrånget till följd av en sådan behandling uppvägas av att passagerarna aktivt medverkar, eftersom det enbart är de själva som har kontroll över lagringen av deras biometriska uppgifter. Om man dessutom beaktar de åtgärder som beskrivs ovan, och förutsatt att den personuppgiftsansvarige vidtar lämpliga skyddsåtgärder i enlighet med kraven för den specifika behandlingen i fråga, kan genomförandet av lämpliga åtgärder säkerställa en lämplig säkerhetsnivå i förhållande till risken. Då kan de negativa konsekvenserna för de registrerades grundläggande rättigheter och friheter anses stå i proportion till den förväntade nyttan.

---

[55] Dataskyddsstyrelsens riktlinjer 5/2022 om ansiktsigenkänning vid brottsbekämpning, punkt 17.

[56] Detta behandlas nedan, från punkt 46.

[57] Detta minimerar till exempel risken för identitetsförfalskning. Se även skyddsåtgärd C.1.2 nedan.

[58] Det skulle också kunna hävdas att den biometriska kontrollen kan vara mindre benägen att göra fel än en mänsklig kontroll.

45. Mot bakgrund av ovanstående drar dataskyddsstyrelsen därför, som svar på fråga 1.1, slutsatsen att sådan behandling **i princip kan anses vara förenlig med artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen, under förutsättning att lämpliga skyddsåtgärder vidtas**.

Lämpliga skyddsåtgärder

46. I denna typ av scenario anser dataskyddsstyrelsen, som svar på fråga 1.2, att åtminstone de skyddsåtgärder som nedan anges bör genomföras. Andra skyddsåtgärder än de som beskrivs i detta yttrande skulle kunna användas för att uppnå samma säkerhets- och dataskyddsmål och vara lagliga så länge de säkerställer att den tillämpliga rättsliga ramen efterlevs.

47. Anmärkning: Detta är en övergripande och icke uttömmande översikt över möjliga lämpliga skyddsåtgärder som den personuppgiftsansvarige bör genomföra i en lösning som liknar scenario 1. Huruvida de är lämpliga enligt artiklarna 25 och 32 i dataskyddsförordningen måste analyseras i varje enskilt fall. Alla personuppgiftsansvariga måste genomföra en egen konsekvensbedömning avseende dataskydd[59] och deras specifika lösningar kan kräva fler åtgärder som inte ingår i detta yttrande.

A. Övergripande skyddsåtgärder

A.1 Konsekvensbedömning avseende uppgiftsbehandling

A.1.1 Genomför en konsekvensbedömning avseende dataskydd, i enlighet med kraven i artikel 35 i dataskyddsförordningen, varje gång den personuppgiftsansvarige planerar en ny behandling som sannolikt kommer att innebära en hög risk. Detta är sannolikt fallet i scenario 1, eftersom det handlar om en behandling av biometriska uppgifter i stor skala[60]. Utvärdera tidigt i utformningsfasen lämpligheten i att införa ett system för ansiktsigenkänning, även med avseende på behovet av ett sådant system och dess proportionalitet i förhållande till de eftersträvade syftena[61], och se över det under hela produktutvecklingens livscykel.

A.1.2 Kontakta den berörda tillsynsmyndigheten om behandlingen fortfarande innebär en hög risk trots de åtgärder som den personuppgiftsansvarige vidtagit för att minimera risken[62].

A.2 De registrerades rättigheter och de skyddsåtgärder som kan genomföras av personuppgiftsansvariga

A.2.1 Skyddsåtgärder för att hantera falska negativa resultat. Minska risken för snedvridningar i fråga om ålder, kön och ras genom att ”regelbundet göra en bedömning av om algoritmerna fungerar i enlighet med syftena och justera algoritmerna för att rätta till systematiska fel

[59] Artikel 35 i dataskyddsförordningen.
[60] Artikel 35.3 i dataskyddsförordningen och artikel 29-arbetsgruppens riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 13 oktober 2017, WP248rev.01, och godkända av dataskyddsstyrelsen.
[61] Artikel 35.7 b i dataskyddsförordningen.
[62] Artikel 36.1 i dataskyddsförordningen.

(biaser) som upptäckts och säkerställa rättvis behandling”[63], till exempel genom mänsklig tillsyn och mänskligt ingripande som ska rätta till eventuella systematiska fel och säkerställa att ingen stigmatisering eller profilering av passagerare förekommer.

A.2.2 Se till att all behandling av personuppgifter sker på ett öppet sätt och att de enskilda personerna är medvetna om att och har kontroll över hur deras uppgifter behandlas under varje behandlingsåtgärd[64].

A.2.3 Säkerställ att åtgärder vidtas som följer principen om ändamålsbegränsning så att uppgifterna inte används för andra ändamål, såsom säkerhets- eller utbildningsändamål.

A.2.4 Se till att lämpliga åtgärder vidtas så att inga fotografier tas och inga videoklipp spelas in, av personer som inte samtycker till ansiktsigenkänning, även om de inte lagras eller behandlas (t.ex. genom lämpligt skärpedjup och lämplig komposition, så att inga bilder tas av andra passagerare i bakgrunden eller runtom, samt med särskilda köer där det tydligt framgår att de avser ansiktsigenkänning).

A.2.5 Vänta på att en passagerare som gett sitt samtycke godtar att ett foto tas eller videoklipp spelas in i de fall samma kontrollenheter kan användas av både passagerare som samtycker till ansiktsigenkänning och passagerare som inte samtycker till ansiktsigenkänning, eller om passagerare som inte samtycker till ansiktsigenkänning kan dyka upp i synfältet medan systemet inte används.

A.2.6 Ge en registrerad person möjligheten att när som helst radera uppgifter som enbart denne lagrar (biometrisk mall[65]) och som finns i en mobilapp eller digital plånbok[66].

A.2.7 Se till att det finns genomförbara alternativ eller backup-lösningar (dvs. för passagerare som inte samtycker till att deras biometriska uppgifter används, för passagerare som inte kan använda sådana lösningar eller för passagerare som fått ett falskt negativt resultat) för att undvika olägenheter för passagerare som inte samtycker[67].

A.2.8 Om en app används bör den vara noggrant utformad och konfigurerad så att inte onödiga uppgifter samlas in och att utvecklingsverktyg för tredjepartsutvecklare, som samlar in data för andra ändamål, inte kan användas.

A.3 Ansvarsskyldighet

[63] Dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, fotnot 60, punkt 70.
[64] Dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 68, och skäl 7 i dataskyddsförordningen.
[65] Hänvisningarna till den biometriska mallen i skyddsåtgärderna för scenario 1 motsvarar hänvisningarna till nyckeln/lösenordet i scenario 2.
[66] Observera att denna skyddsåtgärd endast gäller scenario 1.
[67] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 86.

A.3.1 Kontrollera om det finns några relevanta uppförandekoder eller certifieringsmekanismer som kan hjälpa till att påvisa att behandlingen är säker och förenlig med artikel 32 i dataskyddsförordningen[68]. Kontrollera att åtgärderna är lämpliga för den aktuella behandlingen. Standarder[69], bästa praxis och uppförandekoder, som erkänns av sammanslutningar och andra organ som företräder olika kategorier av personuppgiftsansvariga, kan vara till hjälp när lämpliga åtgärder ska fastställas.

A.3.2 Säkerställ att grundläggande säkerhetskontroller utförs på användarens enhet för att det ska gå att genomföra registreringsfasen, även om passagerarna också har ett ansvar att skydda de uppgifter som lagras på deras enheter. Exempel på sådana tekniska kontroller presenteras nedan i avsnitt C.2 ”Infrastruktur och nätverk”.

B. Organisatoriska skyddsåtgärder:

B.1 Policyer och efterlevnad

B.1.1 Se till att det finns kontroller för den interna tillgången[70] med regler för administratörer.

B.1.2 Om tjänsten för ansiktsigenkänning kan tillhandahållas av en part som deltar i behandlingen utan att de andra berörda parterna behöver hantera några identifieringsuppgifter eller biometriska uppgifter ska det inte vara möjligt att överföra uppgifterna till de parterna. Ett flygbolag behöver till exempel tekniskt sett inte få åtkomst till de biometriska uppgifterna när det använder flygplatsens gemensamma infrastruktur, trots att det är flygbolaget som fungerar som personuppgiftsansvarig för behandlingen enligt dataskyddsförordningen.

B.1.3 Fastställ en policy för kryptering och nyckelhantering[71], till exempel för behandlingen av identifieringsuppgifter och biometriska uppgifter.

B.1.4 Säkerställ att kapitel V i dataskyddsförordningen efterlevs. Till exempel bör det säkerställas att överföringarna uppfyller kraven om den personuppgiftsansvarige under registreringsprocessen använder en fjärrtjänst som är baserad i ett tredjeland.

B.1.5 Säkerställ att det finns ett avtal om personuppgiftsbiträden[72] i enlighet med artikel 28.3 i dataskyddsförordningen när sådana används.

[68] Artikel 32.3 i dataskyddsförordningen och dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 10.
[69] Se t.ex. ISO/IEC 2382–37.
[70] Dataskyddsstyrelsens riktlinjer 4/2020 om användning av lokaliseringsuppgifter och kontaktspårningsverktyg i samband med covid-19-utbrottet, antagna den 21 april 2020 (nedan kallade **dataskyddsstyrelsens riktlinjer 4/2020 om lokaliseringsuppgifter och kontaktspårningsverktyg**), SEC-10, s. 16.
[71] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 89.
[72] Artikel 28.3 i dataskyddsförordningen.

B.1.6 Säkerställ att det finns förfaranden för mänsklig tillsyn och mänskliga ingripanden, i synnerhet för att hantera problem med falska negativa resultat och tekniska problem eller problem med användbarhet.

B.2 Utbildning och testning

B.2.1 Se till att personalen får lämplig utbildning.

B.2.2 Genomför ett ”förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet”[73].

B.2.3 Genomför en process som säkerställer att behandlingen av passagerarens biometriska mall[74] i autentiseringssyfte är effektiv tekniskt sett och korrekt i tillräckligt hög grad.

B.2.4 Säkerställ att de biometriska prover som samlas in vid såväl registreringen som vid kontrollpunkten håller tillräckligt hög kvalitet för att en tillförlitlig biometrisk behandling ska kunna utföras.

C. Tekniska skyddsåtgärder:

C.1 Åtkomst

C.1.1 Genomför skyddsåtgärder under registreringsfasen för att säkerställa att registreringsprocessen självladdas med en verifierad identitet. För att användarnas multifaktoriella identitetsautentisering ska bli ännu starkare kan man till exempel tillämpa lösenordsskyddade engångslänkar för att aktivera appen eller upplåsningsmekanismer på den lokala enheten.

C.1.2 Genomför skyddsåtgärder för att hantera falska positiva resultat och presentationsattacker och förebygga bedrägerier[75].

C.1.3 Förbjud all extern åtkomst till identifieringsuppgifter och biometriska uppgifter[76].

C.1.4 Se till att behandlingen sker lokalt under registrerings-, överförings- och matchningsfaserna. Matchningspunkten bör komma så nära den enskilda personens enhet som möjligt. För att mallar ska kunna matchas på enskilda enheter kan det krävas interaktion

[73] Artikel 32.1 d i dataskyddsförordningen.
[74] Hänvisningarna till den biometriska mallen i skyddsåtgärderna för scenario 1 motsvarar hänvisningarna till nyckeln/lösenordet i scenario 2.
[75] Enisas rapport *Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust* (inte översatt till svenska) från januari 2022.
[76] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 89.

med tjänsteleverantörer utanför flygplatsen och användning av offentliga nätverksresurser, vilket har nackdelen att tillgängligheten kan påverkas och mallen spridas till externa enheter.

C.1.5 Ge en användare behörighet att lägga till en ny flygresa och generera en ny krypterad QR-kod.

C.1.6 Vidta åtgärder för att hantera situationer där en passagerare inte får tillgång till sin QR-kod.

C.2 Infrastruktur och nätverk

C.2.1 Inför krav på att operativsystemen är helt uppdaterade och på autentisering för åtkomst till enheten för att appen eller den digitala plånboken ska fungera, med automatisk radering av identifieringsuppgifter och biometriska uppgifter i händelse av ett gammalt operativsystem som medför säkerhetsrisker.

C.2.2 Se till att matchningsenheterna (dvs. kontrollenheterna) är bortkopplade från nätverk när behandlingen äger rum och att alla andra nödvändiga åtgärder vidtas för att säkerställa säkerheten.

C.2.3 Utför den biometriska matchningen på passagerarens enhet eller på kontrollenheten (kantdatorsystem).

C.2.4 Se till att det finns lösningar som hanterar säkerhetsbrister i passagerarnas egna enheter, däribland kryptering av (åtminstone) biometriska uppgifter och identifieringsuppgifter som inte är aktiva.

C.2.5 Tillämpa säker lagring av (åtminstone) biometriska uppgifter som endast användaren har kontroll över[77], till exempel genom att använda en säker enklav på en smarttelefon.

C.2.6 Vidta åtgärder som säkerställer den fysiska säkerheten i lokalerna, även flygplatsens biometriska terminal. Se till att säkerhetsnivån är hög för de delar av strukturen där identifieringsuppgifter och biometriska uppgifter behandlas (t.ex. beräkningar, dataflöden samt både tillfällig och långvarig lagring).

C.3 Kontroll av användarens identitet, datasäkerhet och datahantering

C.3.1 Dela upp uppgifterna under överföring och lagring i minst tre olika grupper, såsom identifieringsuppgifter, biometriska uppgifter och flyginformation[78]. Säkerställ att uppgifterna krypteras på lämpligt sätt mellan överföring och lagring.

[77] Hänvisningarna till den biometriska mallen i skyddsåtgärderna för scenario 1 motsvarar hänvisningarna till nyckeln/lösenordet i scenario 2.
[78] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 89.

C.3.2 Inrätta tekniska åtgärder för att säkerställa att inga andra uppgifter än de som lagligen kan behandlas vid specifika kontrollpunkter faktiskt behandlas och kontrolleras vid kontrollpunkten.

C.3.3 Säkerställ att raderingen av uppgifterna[79] är effektiv genom ett förfarande för säker radering (vad gäller t.ex. huvudminnet, cacheminnet, potentiella säkerhetskopior) och gör en utvärdering av när raderingen av uppgifterna bör automatiseras. Uppgifternas lagringsperiod bör tillämpas strikt genom automatiska rutiner utan att den enskilda personen behöver vidta några åtgärder[80].

C.3.4 Säkerställ uppgifternas äkthet och integritet (t.ex. med en underskrift)[81].

C.3.5 Lagra passagerarnas biometriska uppgifter vid registreringspunkten och vid kontrollpunkten endast under en mycket kort period och radera dem så snart passagerarna har passerat kontrollpunkten.

C.3.6 Tillämpa säkerhetsstandarder för mobilapplikationssäkerhet under utvecklingen av appen i de fall en app används för registreringen, och låt en tredje part säkerhetstesta den.

C.3.7 Säkerställ att säkerhetsåtgärder vidtas under registreringsfasen på flygplatsen för att bevara konfidentialiteten och integriteten hos passagerarens biometriska uppgifter. Om QR-koden till exempel skrivs ut vid en självbetjäningsautomat bör den inte visas på automatens skärm för att undvika att någon illvillig tar en bild. Vid kortdistansöverföring bör överföringen endast utföras om användaren aktivt medverkar och genom en kanal som säkerställer fysisk närhet.

C.3.8 Uppgifter som enbart den enskilda personen har kontroll över[82] bör förvaras säkert på dennes enhet, och alla sårbarheter som beror på enhetens operativsystem måste rättas till med lämpliga säkerhetsprogramfix. Om QR-koden har skrivits ut bör personen uppmärksammas på att den innehåller särskilt känsliga uppgifter och på vad den kan möjliggöra.

C.3.9 Se till att registreringen görs med hjälp av lämplig teknik som kan styrka identiteten på distans[83].

[79] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 89.
[80] Dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 82.
[81] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 89.
[82] Hänvisningarna till den biometriska mallen i skyddsåtgärderna för scenario 1 motsvarar hänvisningarna till nyckeln/lösenordet i scenario 2.
[83] Se Enisas rapport *Remote ID Proofing: Analysis of methods to carry out identity proofing remotely* (inte översatt till svenska), mars 2021.

3.2.2 Scenario 2: den registrerade biometriska mallen lagras centralt i krypterad form på flygplatsen och med en nyckel eller ett lösenord som endast passageraren har tillgång till, i autentiseringssyfte

48. I detta avsnitt undersöks hur förenligt det är med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen att en passagerares registrerade biometriska mall lagras i en central databas, i krypterad form och med en nyckel eller ett lösenord som endast passageraren har tillgång till, i autentiseringssyfte[84] (nedan kallat **scenario 2**). I detta avsnitt undersöks också lämpliga skyddsåtgärder för scenario 2, mot bakgrund av artiklarna 25 och 32 i dataskyddsförordningen.

Beskrivning av scenariot

49. I scenario 2 görs registreringen endast en gång för en viss giltighetsperiod (t.ex. ett år efter den senaste flygresan, fram till dess att passets giltighetstid löper ut), antingen på distans med lämplig säkerhetsnivå när det gäller identifieringen (t.ex. lämplig eIDAS-säkerhetsnivå) eller på en flygplatsterminal. Registreringen kontrolleras av flygplatsens ledningsenhet och består i att identifieringsuppgifter och biometriska uppgifter genereras och krypteras med en nyckel eller ett lösenord.

50. Databasen förvaras i flygplatsens lokaler och kontrolleras av flygplatsens ledningsenhet. Enskilda personers krypteringsnycklar eller lösenord lagras bara på deras egen enhet (t.ex. i ledningsenhetens mobilapp). Appen kan generera en QR-kod som innehåller nyckeln eller lösenordet och som antingen kan skrivas ut på papper eller visas på enhetens skärm[85]. Flygplatsens ledningsenhet skapar också ett andra krypteringsskikt[86] med nycklar som den har kontroll över.

51. Passagerarna autentiseras (genom en-till-en-verifiering) när de passerar särskilda kontrollpunkter på flygplatsen. De passagerare som väljer att gå igenom de biometriska kontrollpunkterna visar sin QR-kod för en särskild kontrollenhet som är utrustad med en QR-skanner och en kamera. Passagerarens index skickas till databasen med en begäran om den krypterade mallen som då laddas ned och kontrolleras lokalt på kontrollenheten och/eller användarens enhet. Den personuppgiftsansvarige vid kontrollpunkten får bara veta och använda resultatet av matchningen[87].

52. I detta scenario förflyttas inga identifieringsuppgifter eller biometriska uppgifter mellan flygplatser, och det finns ingen sammankoppling eller driftskompatibilitet mellan de centrala databaserna.

Dataskyddsstyrelsens bedömning

53. I scenario 2 lagras passagerarnas registrerade biometriska mallar centralt, men i krypterad form och med en nyckel eller ett lösenord som endast de själva har tillgång till. I scenario 2 autentiseras passagerarna (genom en-till-en-verifiering).

---

[84] Detta exemplifieras genom användningsfall 2 i bilaga I till begäran.
[85] Den franska tillsynsmyndigheten har förtydligat att det kan finnas andra tekniska lösningar som kan användas för att skicka den begärda informationen, t.ex. genom att använda ett protokoll för kortdistanskommunikation.
[86] Nyckeln eller lösenordet (som den enskilda personen har kontroll över) krypteras sedan med en annan nyckel som innehas av flygplatsens ledningsenhet.
[87] Den franska tillsynsmyndigheten klargjorde att denna lagringsperiod är illustrativ och kan anses godtagbar eftersom de enskilda personerna själva har kontroll över nyckeln och kan välja den under registreringsfasen. Det bör dock noteras att lagringsperioden kan ändras.

54. I detta scenario ska målet, det vill säga ett effektivare passagerarflöde (genom snabbare kontroller), uppnås med hjälp av ett centraliserat system. Dataskyddsstyrelsen har tidigare konstaterat att en sådan lösning skulle kunna betraktas som ett genomförbart alternativ till decentraliserad lagring av de registrerade biometriska mallarna[88] (se beskrivningen i scenario 1), om det finns ett objektivt behov av det och om lämpliga skyddsåtgärder (se de skyddsåtgärder som beskrivs i punkt 60 nedan) vidtas.

55. När det gäller säkerheten krypteras varje enskild persons uppgifter med en specifik nyckel som bara personen själv har tillgång till och kontroll över. Den information som krävs för matchningen (dvs. lösenordet eller nyckeln) måste personen dessutom själv tillhandahålla, vilket fungerar som en andra faktor[89] och gör autentiseringen säkrare. Flygplatsens ledningsenhet skapar också ett andra krypteringsskikt med nycklar som den har kontroll över. I scenario 2 skickas enskilda personers index till den centrala databasen för att hämta deras biometriska uppgifter. Dessa uppgifter skickas sedan (krypterade) till en dator vid kontrollpunkten där de dekrypteras i syfte att utföra matchningen, och den personuppgiftsansvarige vid kontrollpunkten får bara veta och använda resultatet av matchningen. Om de personliga nycklarna eller lösenorden förvaras i datorn vid kontrollpunkten, och det bara är passagerarens index som skickas till den centrala databasen för att hämta den krypterade biometriska mallen, kan sådana säkerhetsåtgärder anses vara förenliga med artiklarna 5.1 f och 32 i dataskyddsförordningen.

56. När det gäller förenligheten med artikel 25 i dataskyddsförordningen, och i synnerhet vad gäller att uppfylla kravet på uppgiftsminimering, bör det säkerställas att behandlingen uppfyller nödvändighetsprincipen. I scenario 2 kan de valda åtgärderna anses ha uppfyllt nödvändighetsprincipen i förhållande till det eftersträvade syftet (dvs. att effektivisera passagerarflödet) om den personuppgiftsansvarige kan visa att det inte finns några alternativa lösningar som är mindre inkräktande och kan uppnå samma mål lika effektivt, beroende på omständigheterna kring behandlingen. Även i scenario 2 måste passagerarna visa fram sin enhet[90]. Den personuppgiftsansvarige kan emellertid visa att scenario 2 påskyndar kontrollprocessen jämfört med den nuvarande situationen, där en människa kontrollerar att namnet på boardingkortet stämmer överens med passagerarens identitetshandling[91], eller jämfört med scenario 1. Detta kan naturligtvis inte påvisas om det i dag inte görs några kontroller för att kontrollera passagerarnas identitet med hjälp av deras officiella identitetshandling (se i detta avseende punkt 18 ovan).

57. När det gäller proportionalitetsprincipen kan intrånget i en sådan behandling uppvägas av att passagerarna aktivt medverkar genom att de själva har kontrollen över nyckeln till sina krypterade uppgifter. De säkerhetsrisker som uppstår när passagerarnas biometriska uppgifter lagras i en central databas, men enbart passagerarna själva har tillgång till nyckeln, verkar också kunna minimeras med hjälp av lämpliga skyddsåtgärder (se de skyddsåtgärder som behandlas i punkt 60 nedan). Om man antar att den personuppgiftsansvarige vidtar sådana skyddsåtgärder och följer kraven för den specifika behandlingen i fråga kan riskerna för enskilda personer minimeras, och de negativa konsekvenserna

[88] Dataskyddsstyrelsens riktlinjer 3/2019 om videoenheter, punkt 88.
[89] Detta minimerar till exempel risken för identitetsförfalskning. Se även skyddsåtgärd C.1.2.
[90] Den franska tillsynsmyndigheten har förtydligat att det kan finnas andra alternativ för att visa upp en mall, t.ex. i form av en utskrift. Dataskyddsstyrelsen är också medveten om att man i framtiden skulle kunna överväga annan teknik som bygger på ett NFC-system.
[91] Det skulle också kunna hävdas att den biometriska kontrollen kan vara mindre benägen att göra fel än en mänsklig kontroll.

för de registrerades grundläggande rättigheter och friheter kan då anses stå i proportion till den förväntade nyttan. Naturligtvis bör det i varje enskilt fall säkerställas att endast de uppgifter som behövs för ändamålet behandlas och att bara passagerare som har samtyckt till detta kontrolleras, vilket innebär att det inte får finnas någon risk för att biometriska uppgifter om andra passagerare, som inte har gett sitt samtycke, samlas in.

58. I begäran anges som exempel att lagringstiden för krypterade uppgifter i databasen i scenario 2 som standard kan vara ett år efter personens senaste flygresa och fram till dess att passets giltighetstid löper ut. Det finns ingen information i begäran som styrker en så lång period på grundval av objektiva skäl, men antagligen är det praktiskt med en så lång lagringsperiod med avseende på framtida flygresor. När det gäller lagringsperioden bör de personuppgiftsansvariga kunna motivera varför den är nödvändig för ändamålet i specifika fall om detta scenario ska vara förenligt med artikel 5.1 e i dataskyddsförordningen. Dataskyddsstyrelsen rekommenderar de personuppgiftsansvariga att välja kortast möjliga lagringsperiod, med beaktande av att en del passagerare flyger mycket sällan, och ger de registrerade möjligheten att själva välja vilken lagringsperiod de vill ha.

59. Som svar på fråga 2.1.1 drar dataskyddsstyrelsen därför slutsatsen att sådan behandling **i princip kan anses vara förenlig med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen, under förutsättning att lämpliga skyddsåtgärder vidtas**.

Lämpliga skyddsåtgärder

60. Som svar på fråga 2.1.2 anser dataskyddsstyrelsen att åtminstone följande skyddsåtgärder bör genomföras i denna typ av scenario, **utöver de skyddsåtgärder som förtecknas i scenario 1**. Andra skyddsåtgärder än de som beskrivs i detta yttrande skulle kunna användas för att uppnå samma säkerhets- och dataskyddsmål och vara lagliga så länge de säkerställer att de tillämpliga rättsliga ramarna efterlevs.

61. Anmärkning: *Detta är en övergripande och icke uttömmande översikt över möjliga lämpliga skyddsåtgärder som den personuppgiftsansvarige skulle kunna genomföra i en lösning som liknar scenario 2. Deras lämplighet enligt artiklarna 25 och 32 i dataskyddsförordningen måste analyseras i varje enskilt fall. Alla personuppgiftsansvariga måste säkerställa att de genomför en egen konsekvensbedömning avseende dataskydd, och deras specifika lösningar kan kräva fler åtgärder som inte ingår i detta yttrande.*

D. Övergripande skyddsåtgärder

D.1 De registrerades rättigheter och skyddsåtgärder som kan genomföras av de personuppgiftsansvariga

D.1.1 Se till att passagerarna alltid har kontroll över hur länge deras uppgifter lagras. Lagringsperioderna bör inte vara längre än vad som krävs för det specifika ändamålet. En längsta period bör fastställas till följd av en grundlig analys av olika faktorer såsom identitetshandlingens giltighet. De registrerade bör ges möjligheten att själva välja hur lång lagringsperiod de vill ha, och den bör kunna vara kortare än standardlagringsperioden.

D.1.2 De registrerade bör ha möjlighet att när som helst begära radering av uppgifter som enbart de själva har kontroll över (en nyckel eller ett lösenord) och som lagrats i en mobilapp eller digital plånbok[92].

D.1.3 Se till att den centrala databasen förvaras på ett sätt som gör att den behöriga tillsynsmyndigheten lätt kan utöva tillsyn över den.

E. Organisatoriska skyddsåtgärder:

E.1 Policyer och efterlevnad

E.1.1 Förtroendet för den centrala servern måste vara begränsat. Den centrala servern måste förvaltas enligt tydligt definierade styrningsregler och alla nödvändiga åtgärder måste vidtas för att garantera att den är säker[93].

F. Tekniska skyddsåtgärder:

F.1 Åtkomst

F.1.1 För loggar över vem som har åtkomst till personuppgifter, särskilt identifieringsuppgifter och biometriska uppgifter, och vid vilken tidpunkt åtkomst har skett.

F.2 Infrastruktur och nätverk

F.2.1 Se till att den centrala databasen är korrekt säkrad, även mot tillgänglighetsattacker.

F.2.2 Se till att den centrala databasen, registreringsenheterna och matchningsenheterna inte har någon uppkoppling mot internet. Drift och underhåll (t.ex. säkerhetskopiering, programfix, övervakning osv.) av dessa system ska utföras lokalt inom flygplatsens lokaler.

F.3 Datasäkerhet och datahantering

F.3.1 Använd den senaste kryptografiska tekniken för ett säkert utbyte mellan appen och den centrala servern[94].

[92] Observera att denna skyddsåtgärd endast gäller scenario 2.
[93] Dataskyddsstyrelsens riktlinjer 4/2020 om lokaliseringsuppgifter och kontaktspårningsverktyg, PRIV-5, s. 17.
[94] Dataskyddsstyrelsens riktlinjer 4/2020 om lokaliseringsuppgifter och kontaktspårningsverktyg, SEC-4, s. 16: ”Exempel på tekniker som kan användas: symmetrisk och asymmetrisk kryptering, hashfunktioner, privat medlemskapstest, privata setsnitt, Bloom-filter, insamling av privat information, homomorfisk kryptering”.

F.3.2 Förvara personliga nycklar eller lösenord på den enhet som kommer att användas för dekryptering (dvs. kontrollenheten) och använd inte indexet till något annat än att hämta motsvarande registrerade biometriska mall i den centrala databasen.

F.3.3 Se till att överföringen av nyckeln eller lösenordet mellan användarens enhet och kontrollenheten inte kan avlyssnas eller avläsas eller överföras till tredje part.

F.3.4 Indexera den biometriska mallen när den lagras i den centrala databasen så att autentisering genom en-till-en-verifiering möjliggörs och säkerställ att den är unik och avser rätt person. Säkerställ att indexet inte avslöjar passagerarens identifieringsuppgifter och att det inte har någon korrelation med krypteringsnyckeln.

F.3.5 Autentisera och kryptera all överföring mellan den centrala databasen och kontrollpunkterna på lämpligt vis och se till att den sker på isolerade nätverk.

F.3.6 Undvik dubbelriktade länkar mellan olika dataset (identifieringsuppgifter och biometriska uppgifter samt flyginformation) och ha bara relevanta, enkelriktade länkar i databasen. Ha till exempel endast enkelriktade länkar från index till identifieringsuppgifter, från index till krypterade biometriska uppgifter och från index till flyginformation.

F.3.7 Vidta åtgärder som säkerställer driftskontinuiteten, till exempel genom att ha lämpliga system för backuplagring.

F.3.8 Se till att kontrollenheten inte för loggar över de krypterade eller okrypterade mallarna.

3.2.3 Centraliserad lagring av de registrerade biometriska mallarna i identifieringssyfte

62. I detta avsnitt undersöks hur förenligt det är med artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen att passagerarnas registrerade biometriska mallar lagras centralt, i identifieringssyfte, när sådana mallar inte är krypterade med en nyckel eller ett lösenord som enbart passagerarna själva har kontroll över, i följande två användningsfall: (1) När sådana mallar lagras i en databas inom flygplatsen och kontrolleras av flygplatsens ledningsenhet[95] (nedan kallat **scenario 3.1**), och (2) när sådana mallar lagras i molnet och kontrolleras av flygbolaget[96] (nedan kallat **scenario 3.2**).

63. Dataskyddsstyrelsen anser att användningen av biometriska uppgifter i stora centrala databaser i **identifieringssyfte** inkräktar på de registrerades grundläggande rättigheter och att den skulle kunna leda till allvarliga konsekvenser för de registrerade[97]. Användningen av biometriska uppgifter bör

[95] Detta exemplifieras genom användningsfall 3A i bilaga I till begäran.
[96] Detta exemplifieras genom användningsfall 3B i bilaga I till begäran.
[97] Se till exempel artikel 29-gruppens yttrande 3/2012 om biometrisk teknik, s. 8. Se även punkt 26 ovan.

dessutom granskas i förhållande till det syfte för vilket de behandlas, med avseende på nödvändighets- och proportionalitetsprinciperna[98].

3.2.3.1 Scenario 3.1: centraliserad lagring i en databas inom flygplatsen, under flygplatsens ledningsenhets kontroll

Beskrivning av scenariot

64. I scenario 3.1 lagras passagerarnas registrerade biometriska mall i en central databas i flygplatsens lokaler och kontrolleras av flygplatsens ledningsenhet i krypterad form. Viktigt här är att passagerarnas uppgiftstyper hålls separerade från varandra, vilket innebär att deras identifieringsuppgifter, registrerade biometriska mallar och flyginformation lagras i tre olika databaser. Dessa uppgiftstyper krypteras med olika nycklar, både under lagringen och under överföringen till de servrar som utför matchningen, där de sedan dekrypteras av flygplatsens ledningsenhet.

65. Passagerarna måste registrera sig för varje flygresa en kort tid före avresan (t.ex. 48 timmar). Detta kan antingen utföras på distans eller på flygplatsterminalen med lämplig säkerhetsnivå när det gäller identifieringen (t.ex. lämplig eIDAS-säkerhetsnivå). Registreringen skulle också kunna ske på samma sätt som beskrivs i scenario 1, där passagerarna måste skicka uppgifterna från sina digitala plånböcker till flygplatsens system inom en tidsram på 48 timmar före avresan.

66. Även i detta scenario ska passagerarna visa upp sig för en särskild kontrollenhet utrustad med en kamera. Deras biometriska prov skickas sedan till en central flygplatsserver som försöker matcha det mot uppgifterna i den centrala biometriska databasen. Passagerarna kan då identifieras och det kan kontrolleras om de verkligen är registrerade för ett avgående flyg (eller det flyg de just ska gå ombord på, om kontrollen sker vid ombordstigning). Beroende på vilken kontrollpunkten är kan de uppgifter som skickas tillbaka till den personuppgiftsansvarige för kontrollpunkten minimeras, till exempel som ”ja/nej-svar” eller själva matchningsresultatet, om så krävs. I detta fall överförs endast resultatet av begäran till den personuppgiftsansvarige vid kontrollpunkten som sen använder det.

67. I detta scenario identifieras passagerarna (genom en-till-N-verifiering), där N är det antal passagerare som förväntas på flygplatsen inom en flera dagar lång tidsram. Den biometriska matchningen sker dessutom bara då passageraren infinner sig på förhand angivna kontrollpunkter på den flygplats varifrån flyget avgår, men själva behandlingen av uppgifterna sker på en central server som är ansluten till den centrala databasen. Lagringsperioden i detta scenario är vanligtvis 48 timmar och uppgifterna raderas så snart planet har startat.

Dataskyddsstyrelsens bedömning

68. Som tidigare nämnts medför behandlingen av biometriska uppgifter ökade risker för de registrerades rättigheter och friheter[99]. Varje lucka i datasäkerheten kan därför få särskilt allvarliga konsekvenser för de registrerade[100]. De personuppgiftsansvariga är skyldiga att effektivt minimera dessa risker.

[98] Skäl 4 i dataskyddsförordningen. Se även artikel 29-arbetsgruppens yttrande 3/2012 om biometrisk teknik, s. 8.
[99] Se punkt 26 ovan.
[100] *Guidelines on facial recognition* (inte översatt till svenska) från rådgivande kommittén för Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, juni 2021, s. 22.

Eftersom hela strukturen i detta scenario är fullständigt centraliserad tappar passagerarna i högre grad kontrollen över sina uppgifter. Utöver detta kan risken vara större för att uppgifterna behandlas för andra ändamål än att kontrollera passagerarflödet.

69. Mot bakgrund av principen om och kraven på säkerhet (artiklarna 5.1 f och 32 i dataskyddsförordningen) bör det beaktas att lagring av identifieringsuppgifter och biometriska uppgifter i centrala databaser kan ge höga angreppsvärden, även om databaserna är separata, och att konfidentialitetsbrott i en sådan databas kan ge åtkomst till hela datasetet. Följden av en eventuell incident när det gäller mallarna för ansiktsigenkänning och tillhörande identifieringsuppgifter kan bli att obehörig eller olaglig identifiering av de registrerade i andra miljöer möjliggörs. Det kan också, beroende på vilka metoder för biometrisk identifiering som används, medföra att annan säker användning av mallarna för ansiktsigenkänning som kännetecken hotas. I sådana fall kan inte konsekvenserna av incidenten minimeras, till skillnad från när det gäller andra typer av åtkomstuppgifter (t.ex. ett användarnamn eller lösenord) som kan ändras[101].

70. Den stora mängden av och höga kvaliteten på de identifieringsuppgifter och biometriska uppgifter som den personuppgiftsansvarige har tillgång till gör dem dessutom till ett mycket värdefullt mål för en angripare, vilket ökar sannolikheten sett till säkerhetsrisker. Uppgiftsincidenter skulle också kunna få större inverkan eftersom en angripare lättare kan få tillgång till personuppgifter som rör flera passagerare när de lagras centralt. En eventuell incident skulle därför kunna utsätta ett stort antal registrerade för stora och allvarliga risker, till exempel identitetsstöld i stor skala, som är extremt svåra att minimera.

71. När det gäller förenligheten med artiklarna 5.1 f och 32 i dataskyddsförordningen är således de åtgärder som planeras i scenario 3.1[102], med hänsyn till dagens teknik, inte tillräckliga för att säkerställa att säkerhetsnivån motsvarar riskerna. Behandlingen enligt scenario 3.1 skulle således inte vara förenlig med artikel 5.1 f eller artikel 32 i dataskyddsförordningen om den personuppgiftsansvarige enbart vidtar dessa åtgärder.

72. Lagringsperioden för biometriska uppgifter i den centrala databasen är vanligtvis 48 timmar i detta scenario, vilket bör ses mot bakgrund av principen i artikel 5.1 e i dataskyddsförordningen. Denna lagringsminimering verkar avsevärt minska de risker som följer av personuppgiftsincidenter. Uppgifternas lagringsperiod är dock inte i sig själv en avgörande faktor för denna strukturs efterlevnad av principen, eftersom den kan ändras av de personuppgiftsansvariga. Dessutom måste de föreslagna åtgärderna under alla omständigheter uppfylla kraven på inbyggt dataskydd och dataskydd som standard enligt artikel 25 i dataskyddsförordningen.

73. Till skillnad från i scenarierna 1 och 2, där passagerarna autentiseras, identifieras passagerarna i scenario 3.1 (genom en-till-N-verifiering), där N är det antal passagerare som förväntas röra sig på flygplatsen inom en tidsram på flera dagar och som har samtyckt till att behandlas när de passerar särskilda kontrollpunkter vid flygplatsen. Detta innebär att en sökning görs efter passagerare i en central databas där varje biometriskt prov som samlas in behandlas för att kontrollera om det stämmer överens med någon känd person i systemet. Till skillnad från i scenario 2 är det inte enbart passagerarna själva som har kontroll över nycklarna i scenario 3.1. I detta scenario har passagerarna

[101] Se i detta avseende artikel 29-arbetsgruppens yttrande 3/2012 om biometrisk teknik, s.34.
[102] Såsom beskrivs i punkterna 64–67 ovan.

följaktligen betydligt mindre kontroll över sina biometriska uppgifter. Den behandling som föreslås i scenario 3.1 kan därför inte vara förenlig med kraven på inbyggt dataskydd och på utformning enligt artikel 25 i dataskyddsförordningen.

74. I enlighet med artikel 25 i dataskyddsförordningen bör de personuppgiftsansvariga beakta typerna, kategorierna och detaljnivån för de personuppgifter som krävs för ändamålet med behandlingen[103]. När de väljer hur utformningen ska se ut bör de ta hänsyn till de ökade riskerna vad gäller principerna om uppgiftsminimering, integritet och konfidentialitet och lagringsminimering när stora mängder detaljerade personuppgifter samlas in, och jämföra dem med de mindre riskerna när mindre mängder och/eller mindre detaljerad information om de registrerade samlas in. Under inga omständigheter bör standardinställningen innebära att personuppgifter samlas in som inte är nödvändiga för det specifika ändamålet med behandlingen. Om vissa kategorier av personuppgifter är onödiga, eller om detaljerade uppgifter inte behövs eftersom det räcker med mindre detaljerade, bör eventuella överflödiga personuppgifter alltså inte samlas in. I detta fall betyder det att man inte behöver använda ansiktsigenkänningstekniken eftersom en annan behandling kan uppnå samma mål och finns tillgänglig i enlighet med vad som beskrivs i scenario 3.1.

75. När det gäller artikel 25 i dataskyddsförordningen är den registrerades självbestämmande ett centralt begrepp för att skydda uppgifter genom inbyggt dataskydd och dataskydd som standard. I synnerhet bör de registrerade ges största möjliga självbestämmande när det gäller att avgöra hur deras personuppgifter ska användas, samt i fråga om användningens eller behandlingens omfattning och villkor[104]. I scenario 1 skulle de registrerade ha självbestämmande och kontroll över hur deras biometriska mallar används, lämnas ut och raderas, och i scenario 2 skulle de behålla viss kontroll över hur den egna biometriska mallen lämnas ut, eftersom det är de som har kontroll över krypteringsnyckeln eller lösenordet. I scenario 3.1 är de registrerade dock helt beroende av den personuppgiftsansvariges val när det gäller hur deras biometriska uppgifter ska behandlas och de har därför ingen direkt kontroll över hur deras biometriska mall används.

76. När det gäller förenligheten med artikel 25 i dataskyddsförordningen anses den behandling som avses i scenario 3.1 inte uppfylla nödvändighetsprincipen, och särskilt inte kravet på uppgiftsminimering. Dataskyddsstyrelsen anser att passagerarflödet på flygplatser kan bli mer eller mindre lika effektivt på ett mindre integritetskränkande sätt, till exempel utan att biometriska uppgifter används (även om användarnas upplevelse förvisso inte blir densamma, då det kan ta längre tid att visa boardingkort och, när så krävs, officiella identitetshandlingar). Andra lösningar, framför allt sådana som bygger på att de biometriska uppgifterna ska lagras i en plånbok på enskilda personers egna enheter eller att uppgifterna ska krypteras med en specifik nyckel som personen har på sin enhet, gör det dessutom möjligt att uppnå målen på ett mindre integritetskränkande sätt.

77. När det gäller proportionalitetsprincipen skulle behandlingen i scenario 3.1 skapa risker för de registrerades rättigheter som med dagens teknik inte kan minimeras genom de planerade skyddsåtgärderna. Risken för att de registrerades grundläggande rättigheter och friheter påverkas negativt till följd av en uppgiftsincident i en central databas där många personers biometriska uppgifter lagras i molnet verkar vara större än den förväntade nyttan av behandlingen. Nyttan är

[103] Dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 49.
[104] Dataskyddsstyrelsens riktlinjer 4/2019 om inbyggt dataskydd och dataskydd som standard, punkt 70. I skäl 7 i dataskyddsförordningen klargörs också att ”[f]ysiska personer bör ha kontroll över sina egna personuppgifter”.

nämligen relativt liten, det vill säga att kontrollerna blir lite bekvämare och går lite snabbare. Det kan därmed inte motiveras att dessa åtgärder i hög grad inkräktar på enskilda personers grundläggande rättigheter och friheter, och den behandling som avses i scenario 3.1 är således inte förenlig med proportionalitetsprincipen.

78. Som svar på fråga 2.2.1 drar därför dataskyddsstyrelsen slutsatsen att den behandling som planeras i scenario 3.1, i det särskilda syftet att effektivisera passagerarflödet på flygplatser,

- **inte kan vara förenlig med artikel 25 i dataskyddsförordningen**,
- **inte skulle vara förenlig med artikel 5.1 f eller artikel 32 i dataskyddsförordningen** om den personuppgiftsansvarige enbart vidtar de åtgärder som beskrivs i scenario 3.1.

3.2.3.2 Scenario 3.2: centraliserad lagring i ett moln, under flygbolagets kontroll

Beskrivning av scenariot

79. I scenario 3.2 lagras passagerarnas registrerade biometriska mall i molnet, under flygbolagets eller dess molntjänstleverantörs (personuppgiftsbiträdes) kontroll. Enligt begäran skulle molntjänstleverantören vara etablerad inom EES[105]. I detta fall krypteras passagerarnas uppgifter men dekrypteras när de används (t.ex. när matchningen utförs), och nycklarna kontrolleras av flygbolaget eller dess personuppgiftsbiträde. Passagerarnas biometriska uppgifter används för att identifiera dem (genom en-till-N-verifiering), där N kan vara upp till alla flygbolagets kunder[106].

80. Liksom i scenarierna 1, 2 och 3.1 måste passagerarna även här först registrera sig. I scenario 3.2 görs dock registreringen en enda gång och finns kvar så länge kunden har ett konto hos flygbolaget. Den görs antingen på distans med lämplig säkerhetsnivå när det gäller identifieringen (t.ex. lämplig eIDAS-säkerhetsnivå) eller på en flygplatsterminal. Den biometriska matchningen sker bara då passagerarna visar sig för på förhand angivna kontrollpunkter på flygplatsen, men själva databehandlingen sker i molnet.

81. På flygplatsen går passagerarna igenom särskilda kontrollenheter som är utrustade med en kamera. Deras biometriska uppgifter skickas genom en begäran till flygbolagets molnserver, där de matchas mot den centrala databasen. Passagerarna kan då identifieras och det kan kontrolleras om de verkligen är registrerade för ett avgående flyg (eller det flyg de just ska gå ombord på, om kontrollen sker vid ombordstigning).

82. Flera ledningsenheter skulle kunna få tillgång till matchningsresultaten på de flygplatser där ett flygbolag har en särskild terminal eller tillgång till flygplatsernas gemensamma infrastruktur för informationssystem. Beroende på vilken kontrollpunkten är kan de uppgifter som skickas tillbaka till den personuppgiftsansvarige för kontrollpunkten minimeras, till exempel som ”ja/nej-svar” eller själva matchningsresultatet, om så krävs. I det här fallet får den personuppgiftsansvarige vid kontrollpunkten bara veta och använda resultatet av begäran.

83. Det är flygbolaget som bestämmer hur länge mallen ska lagras, och det skulle kunna vara så länge kunden har ett konto hos flygbolaget.

Dataskyddsstyrelsens bedömning

84. De överväganden som dataskyddsstyrelsen redan framfört för scenario 3.1[107] gäller även för detta scenario.

85. När det gäller principen om och kraven på säkerhet (artiklarna 5.1 f och 32 i dataskyddsförordningen) sker behandlingen i scenario 3.2 i molnet och flera enheter kan få tillgång till uppgifterna, eventuellt

[105] Den franska tillsynsmyndigheten förtydligade att detta är ett exempel och att molntjänstleverantörer som inte är etablerade i EES också kan övervägas. Även andra lagringslösningar (t.ex. utan moln) skulle kunna övervägas.
[106] Den franska tillsynsmyndigheten förtydligade att detta är ett exempel och att det finns en lösning där de biometriska uppgifterna skickas innan varje enskild flygresa.
[107] Punkterna 68–77 ovan.

även leverantörer utanför EES till och med då uppgifterna lagras inom EES[108]. En sådan struktur skapar potentiella risker för att personuppgifterna överförs till tredjeländer. Passagerarnas uppgifter krypteras förvisso, men de dekrypteras när de används (dvs. när matchningen utförs) och det är flygbolaget eller dess personuppgiftsbiträde för molnet som kontrollerar nycklarna. När de lagras på det här sättet kan angreppsytan bli ännu större.

86. När det gäller förenligheten med artiklarna 5.1 f och 32 i dataskyddsförordningen är de åtgärder som planeras i scenario 3.2[109] därför, med dagens teknik, otillräckliga när det gäller att säkerställa en lämplig säkerhetsnivå i förhållande till risken. Behandlingen enligt scenario 3.2 skulle således inte vara förenlig med artikel 5.1 f eller artikel 32 i dataskyddsförordningen om den personuppgiftsansvarige enbart vidtar dessa åtgärder.

87. I scenario 3.2[110] kan uppgifterna dessutom lagras under en lång period (potentiellt så länge som den registrerade har ett konto hos flygbolaget). En så lång lagringstid gör att risken för att deras konfidentialitet och integritet bryts blir större än vad som är absolut nödvändigt och proportionerligt för ändamålen med behandlingen. Dataskyddsstyrelsen noterar att datalagringsperioden inte i sig själv är avgörande för denna strukturs övergripande förenlighet med dataskyddsförordningen, eftersom de personuppgiftsansvariga kan ändra längden på perioden. I den information som dataskyddsstyrelsen har tillgång till och som ingår i beskrivningen av scenario 3.2 finns det dock inget som motiverar en så lång lagringstid och inga uppenbara åtgärder som minimerar riskerna för enskilda personer. Den lagringsperiod som föreslagits är alltså inte begränsad till vad som är nödvändigt i enlighet med principen om lagringsminimering i artikel 5.1 e i dataskyddsförordningen.

88. Under inga omständigheter kan de åtgärder som föreslagits i scenario 3.2 anses uppfylla kraven på inbyggt dataskydd och på utformning enligt artikel 25 i dataskyddsförordningen. I scenario 3.2 lagras passagerarnas registrerade biometriska mallar i molnet under flygbolagets eller dess molntjänstleverantörs (personuppgiftsbiträdes) kontroll. Som beskrivits ovan är det möjligt att fler enheter skulle kunna få tillgång till dessa uppgifter. Dessutom används passagerarnas biometriska uppgifter för att identifiera dem (genom en-till-N-verifiering), där N kan vara upp till alla flygbolagets användare och kunder. En sådan metod innebär att en person ska hittas bland en grupp personer i den centrala databasen genom att varje ansiktsbild behandlas för att kontrollera om den stämmer överens med någon känd person i systemet. Till skillnad från i scenario 3.1 skulle jämförelsen i scenario 3.2 kunna göras i mycket större skala eftersom kriteriet här är alla flygbolagets kunder, medan scenario 3.1 endast omfattade det antal passagerare som förväntades inom en tidsram på några dagar.

89. När det gäller förenligheten med artikel 25 i dataskyddsförordningen, och i synnerhet kravet på uppgiftsminimering, kan den behandling som avses i scenario 3.2 inte heller anses uppfylla nödvändighetsprincipen. Dataskyddsstyrelsen anser att passagerarflödet på flygplatser kan bli mer eller mindre lika effektivt på ett mindre integritetskränkande sätt, till exempel utan att biometriska uppgifter används, även om användarnas upplevelse inte blir densamma då det kan ta längre tid att visa id-handlingen och boardingkortet. Andra lösningar kan dessutom göra att den

[108] Dataskyddsstyrelsen 2022, *Coordinated Enforcement Action on the use of cloud-based services by the public sector* (inte översatt till svenska) från den 17 januari 2023, s. 19.
[109] Se punkterna 79–83 ovan.
[110] Se punkt 83 ovan.

personuppgiftsansvarige kan uppnå målen på ett mindre integritetskränkande sätt, framför allt lösningar som bygger på att de biometriska uppgifterna lagras i en plånbok på enskilda personers enheter eller att uppgifterna krypteras med en specifik nyckel som varje person har på den egna enheten.

90. När det gäller proportionalitetsprincipen skulle behandlingen i scenario 3.2 skapa risker för de registrerades rättigheter som inte kan minimeras genom de planerade skyddsåtgärderna. De negativa konsekvenserna för de registrerades grundläggande rättigheter och friheter vid en uppgiftsincident i en central databas, som innehåller många personers biometriska uppgifter och som lagras i molnet, tycks större än den förväntade nyttan av behandlingen. Nyttan är nämligen relativt liten, det vill säga att kontrollerna blir lite bekvämare och går lite snabbare. Det kan därmed inte motiveras att dessa åtgärder i hög grad inkräktar på enskildas grundläggande rättigheter och friheter, och den behandling som avses i scenario 3.2 kan således inte anses vara proportionerlig.

91. Som svar på fråga 2.3.1 drar dataskyddsstyrelsen därför slutsatsen att den behandling som planeras i scenario 3.2, i det särskilda syftet att effektivisera passagerarflödet på flygplatser,

- **inte kan vara förenlig med artikel 25 i dataskyddsförordningen**,
- **inte skulle vara förenlig med artikel 5.1 f eller artikel 32 i dataskyddsförordningen** om den personuppgiftsansvarige enbart vidtar de åtgärder som beskrivs i scenario 3.2,
- **inte är förenlig med artikel 5.1 e i dataskyddsförordningen**, eftersom det inte finns något som motiverar en så lång lagringstid som den som anges i scenario 3.2, utifrån den information som dataskyddsstyrelsen har tillgång till. Om principen om lagringsminimering i artikel 5.1 e i dataskyddsförordningen ska uppfyllas måste den personuppgiftsansvarige kunna visa att personuppgifterna inte lagras längre än vad som är nödvändigt för de ändamål för vilka de behandlas.

4 SLUTSATSER

92. När det gäller fråga 1.1 drar dataskyddsstyrelsen, efter en begäran om ett yttrande från den franska tillsynsmyndigheten, följande slutsats med avseende på kraven i artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen och på grundval av analysen ovan:

93. Användningen av ansiktsigenkänningsteknik för biometrisk autentisering i det specifika syftet att effektivisera passagerarflödet på flygplatser (vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger) med hjälp av en lagringsstruktur där varje passagerare har kontroll över sin registrerade biometriska mall, eftersom den lagras lokalt på personens egen enhet, i princip skulle kunna anses vara förenlig med principerna om integritet och konfidentialitet enligt artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen om lämpliga skyddsåtgärder vidtas enligt punkt 46 ovan.

94. När det gäller fråga 2.1.1 drar dataskyddsstyrelsen, efter en begäran från den franska tillsynsmyndighetens begäran om ett yttrande avseende kraven i artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen och på grundval av analysen ovan, följande slutsatser:

95. Användningen av ansiktsigenkänningsteknik för biometrisk autentisering i det specifika syftet att effektivisera passagerarflödet på flygplatser (vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger) med hjälp av en central lagringsstruktur, där varje

passagerares registrerade biometriska mall lagras i en central databas inom flygplatsen, som kontrolleras av flygplatsens ledningsenhet, i krypterad form och med en nyckel eller ett lösenord som endast den registrerade har tillgång till, i princip skulle kunna anses vara förenlig med principen om lagringsminimering enligt artikel 5.1 e och principerna om integritet och konfidentialitet enligt artiklarna 5.1 f, 25 och 32 i dataskyddsförordningen, om lämpliga skyddsåtgärder vidtas enligt punkt 60 ovan.

96. När det gäller fråga 2.2.1 drar dataskyddsstyrelsen, efter en begäran från den franska tillsynsmyndigheten om ett yttrande avseende kraven i artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen och på grundval av analysen ovan, följande slutsatser

97. Användningen av ansiktsigenkänningsteknik för biometrisk autentisering i det specifika syftet att effektivisera passagerarflödet på flygplatser (vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger) med hjälp av en central lagringsstruktur, där passagerarnas registrerade biometriska mallar lagras i en databas på flygplatsen och kontrolleras av flygplatsens ledningsenhet men inte krypteras med en nyckel eller ett lösenord som endast passageraren själv har tillgång till, inte är förenlig med artikel 25 i dataskyddsförordningen. En sådan behandling skulle inte heller vara förenlig med principen om integritet och konfidentialitet enligt artiklarna 5.1 f och 32 i dataskyddsförordningen om den personuppgiftsansvarige enbart vidtar de åtgärder som beskrivs i scenario 3.1.

98. När det gäller fråga 2.3.1 drar dataskyddsstyrelsen, efter en begäran från den franska tillsynsmyndigheten om ett yttrande avseende kraven i artikel 5.1 e och f samt artiklarna 25 och 32 i dataskyddsförordningen och på grundval av analysen ovan, följande slutsatser

99. Användningen av ansiktsigenkänningsteknik för biometrisk autentisering i det specifika syftet att effektivisera passagerarflödet på flygplatser (vid säkerhetskontroller, bagageinlämning, ombordstigning och tillträde till passagerarlounger) med hjälp av en central lagringsstruktur, där passagerarnas registrerade biometriska mallar lagras i molnet och kontrolleras av flygbolaget men inte krypteras med en nyckel eller ett lösenord som endast passageraren själv har tillgång till, är inte förenlig med artikel 25 i dataskyddsförordningen. En sådan behandling skulle inte heller vara förenlig med principerna om integritet och konfidentialitet enligt artiklarna 5.1 f och 32 i dataskyddsförordningen om den personuppgiftsansvarige enbart vidtar de åtgärder som beskrivs i scenario 3.2. Slutligen, på grundval av beskrivningen av scenario 3.2 och den information som dataskyddsstyrelsen har tillgång, är behandlingen inte heller förenlig med principen om lagringsminimering enligt artikel 5.1 e i dataskyddsförordningen.

För Europeiska dataskyddsstyrelsen

Ordförande

(Anu Talus)