Udtalelse 11/2024 om anvendelse af ansigtsgenkendelse til at strømline passagerstrømmen i lufthavne (forenelighed med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR)

Udgave 1.1

Vedtaget 23. maj 2024

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

Vedtaget

Udgave 1.1	28. maj 2024	Grammatisk korrektion i resuméet (side 3 og 4) og punkt 77 og 90 i udtalelsen
Udgave 1.0	23. maj 2024	Vedtagelse af udtalelsen

Resumé

Den franske tilsynsmyndighed anmodede Det Europæiske Databeskyttelsesråd om at afgive en udtalelse om lufthavnsoperatørers og luftfartsselskabers brug af ansigtsgenkendelsesteknologi til biometrisk autentifikation eller identifikation af passagerer for at strømline passagerstrømmen i lufthavne.

Indledningsvis minder Databeskyttelsesrådet om, at anvendelsen af biometriske data og navnlig ansigtsgenkendelsesteknologi indebærer øgede risici for de registreredes rettigheder og frihedsrettigheder. Den vedrører behandling af biometriske data, som er omfattet af særlig beskyttelse i henhold til artikel 9 i GDPR. Inden sådanne teknologier anvendes, bør de dataansvarlige, selv om teknologierne anses for at være særligt effektive, vurdere indvirkningen på de registreredes grundlæggende rettigheder og frihedsrettigheder og overveje, om mindre indgribende midler kan opfylde deres legitime formål med behandlingen.

Omfanget af denne udtalelse er, som det fremgår af anmodningen, begrænset til behandlingens forenelighed med **artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR** for det **specifikke formål at strømline passagerstrømmen i lufthavne** ved fire specifikke kontrolsteder, nemlig ved sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge. Denne udtalelse indeholder ikke en fuldstændig analyse af de relevante dataansvarliges og deres eventuelle databehandleres overholdelse af GDPR i hvert enkelt tilfælde. Denne udtalelse berører derfor ikke en juridisk og teknisk analyse i en given sag baseret på en dataansvarligs specifikke påtænkte behandling og omstændigheder. Analysen af det gældende retsgrundlag er desuden ikke omfattet af de spørgsmål, der er forelagt Databeskyttelsesrådet i anmodningen, og som følge heraf undersøges gyldigheden af samtykke til en sådan behandling i overensstemmelse med artikel 6, 7 og 9 i GDPR ikke i denne udtalelse. Denne udtalelse berører desuden ikke de begrænsninger for anvendelsen af biometriske data, der er fastsat i medlemsstaternes lovgivning.

I denne udtalelse vurderer Databeskyttelsesrådet, om behandlingen er i overensstemmelse med ovennævnte bestemmelser i GDPR i forbindelse med **fire konkrete scenarier**.

Det **første scenarie** indebærer opbevaring af en registreret biometrisk skabelon hos den enkelte, f.eks. på vedkommendes individuelle enhed, under vedkommendes enekontrol med henblik på at autentificere passageren (1:1-sammenligning), når vedkommende går gennem ovennævnte kontrolsteder i lufthavnen.

Databeskyttelsesrådet konkluderer, at de valgte foranstaltninger kan anses for at have opfyldt nødvendighedsprincippet, hvis den dataansvarlige kan påvise, at der ikke findes mindre indgribende alternative løsninger, der kan nå det samme mål lige så effektivt. Behandlingens indgribende karakter kan desuden opvejes af passagerernes aktive inddragelse, da deres biometriske skabelon kun lagres hos dem, f.eks. på deres individuelle enhed, under deres enekontrol, og deres oplysninger slettes kort efter, at matchningen er afsluttet. På dette grundlag konkluderer Databeskyttelsesrådet, at den behandling, der er påtænkt i det første scenarie, **i princippet kan anses for at være forenelig med artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR** med forbehold af gennemførelsen af de fornødne garantier.

Databeskyttelsesrådet har identificeret de garantier, der som minimum bør gennemføres for en løsning, der svarer til det første scenarie.

Det **andet scenarie** indebærer central lagring i lufthavnen af en registreret biometrisk skabelon i krypteret form med en nøgle/hemmelighed, der udelukkende er i passagerens hænder. Dette muliggør passagerautentifikation (1:1-sammenligning), når de passerer gennem de ovennævnte kontrolsteder i lufthavnen. Registreringen er gyldig i en given periode, som f.eks. kan være op til et år efter den sidste flyvning frem til passets udløbsdato.

Databeskyttelsesrådet konkluderer, at behandlingen kan anses for at have opfyldt nødvendighedsprincippet, hvis den dataansvarlige kan påvise, at der ikke findes mindre indgribende alternative løsninger, der kan nå det samme mål lige så effektivt. Behandlingens indgribende karakter kan desuden opvejes af den aktive inddragelse af passageren, da denne opbevarer nøglen/hemmeligheden til sine krypterede biometriske data under vedkommendes enekontrol. Forudsat at den dataansvarlige gennemfører de fornødne garantier, kan sikkerhedsrisiciene afbødes ved at anvende en central database i dette scenarie, og den negative indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder kan anses for at stå i et rimeligt forhold til den forventede fordel. Med hensyn til princippet om opbevaringsbegrænsning er der ikke blevet fremlagt oplysninger for Databeskyttelsesrådet, der underbygger den lange opbevaringsperiode. For at opnå forenelighed med artikel 5, stk. 1, litra e), i GDPR i dette scenarie bør de dataansvarlige kunne begrunde, hvorfor den påtænkte opbevaringsperiode er nødvendig til formålet i specifikke tilfælde. Databeskyttelsesrådet anbefaler, at de dataansvarlige overvejer den kortest mulige opbevaringsperiode og samtidig giver passagererne mulighed for at fastsætte deres foretrukne opbevaringsperiode. På dette grundlag konkluderer Databeskyttelsesrådet, at den behandling, der er påtænkt i det andet scenarie, **i princippet kan anses for at være forenelig med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR** med forbehold af gennemførelsen af de fornødne garantier.

Databeskyttelsesrådet har identificeret de garantier, der som minimum bør gennemføres for en løsning, der svarer til det andet scenarie.

Det **tredje scenarie** indebærer central lagring af en registreret biometrisk skabelon i krypteret form i lufthavnen under lufthavnsoperatørens kontrol. Dette muliggør passageridentifikation (1:N-sammenligning), når de passerer gennem de ovennævnte kontrolsteder i lufthavnen. Opbevaringsperioden i dette scenarie er typisk 48 timer, og dataene slettes, når flyet er lettet.

Da identifikationsdata og biometriske data lagres i en central database, kan det, hvis databasens fortrolighed kompromitteres, efterfølgende medføre adgang til hele datasættet og muliggøre uautoriseret eller ulovlig identifikation af passagerer i andre miljøer. Den centraliserede lagringsarkitektur, der kontrolleres af lufthavnsoperatøren, medfører også, at passagerne i højere grad mister kontrollen over deres oplysninger. Databeskyttelsesrådet mener, at et resultat, der svarer til strømlining af passagerstrømmen i lufthavne, kan opnås på en mindre indgribende måde, og at den negative indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder, der kan følge af et brud på datasikkerheden i en central database med biometriske data, synes at opveje de forventede fordele ved behandlingen. Behandlingen kan derfor ikke anses for at opfylde nødvendigheds- og proportionalitetsprincipperne. På dette grundlag konkluderer Databeskyttelsesrådet, at den behandling, der er påtænkt i det tredje scenarie, **ikke kan anses for at være forenelig med artikel 25 i GDPR**. Det **er desuden ikke i overensstemmelse med artikel 5, stk. 1, litra f), og artikel 32 i GDPR**, hvis en dataansvarlig begrænser sig til de foranstaltninger, der er beskrevet i dette scenarie.

Det **fjerde scenarie** indebærer central lagring af en registreret biometrisk skabelon i krypteret form i skyen under luftfartsselskabets eller dets cloudtjenesteudbyders kontrol. Dette muliggør passageridentifikation (1:N-sammenligning), når de passerer gennem de ovennævnte kontrolsteder i

lufthavnen. Opbevaringsperioden i dette scenarie kan potentielt være, så længe kunden har en konto hos luftfartsselskabet.

Da identifikationsdata og biometriske data lagres i en central database i skyen, kan flere enheder have adgang til disse data, herunder eventuelt udbydere uden for EØS. Passagerens data dekrypteres, når de er i brug, og nøglerne er under luftfartsselskabets eller dets databehandleres kontrol, hvilket kan øge den sikkerhedsmæssige eksponering. En sådan centraliseret lagringsarkitektur medfører også, at passagererne i højere grad mister kontrollen over deres oplysninger. Dataene kan også lagres i en betydelig periode. De er derfor udsat for en større risiko for sikkerhedsbrud, som tilsyneladende går ud over, hvad der er strengt nødvendigt og forholdsmæssigt med henblik på behandlingen, medmindre der træffes yderligere åbenbare foranstaltninger for at mindske risiciene for enkeltpersoner.

Databeskyttelsesrådet mener, at et resultat, der svarer til strømlining af passagerstrømmen i lufthavne, kan opnås på en mindre indgribende måde, og at den negative indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder, der kan følge af et brud på datasikkerheden i en central database med biometriske data, synes at opveje de forventede fordele ved behandlingen. Behandlingen kan derfor ikke anses for at opfylde nødvendigheds- og proportionalitetsprincipperne. På dette grundlag konkluderer Databeskyttelsesrådet, at den behandling, der er påtænkt i det fjerde scenarie, **ikke kan anses for at være forenelig med artikel 25 i GDPR**. På grundlag af de oplysninger, der er til rådighed for Databeskyttelsesrådet, er det desuden **ikke i overensstemmelse med artikel 5, stk. 1, litra e), i GDPR** samt **artikel 5, stk. 1, litra f), og artikel 32 i GDPR**, hvis en dataansvarlig begrænser sig til de foranstaltninger, der er beskrevet i dette scenarie.

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har –

under henvisning til artikel 63 og artikel 64, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF ("**GDPR**"),

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS), særlig bilag XI og protokol 37 som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018[1], og

under henvisning til artikel 10 og 22 i forretningsordenen for Det Europæiske Databeskyttelsesråd ("**Databeskyttelsesrådet**" eller "**EDPB**") ("**Databeskyttelsesrådets forretningsorden**"),

ud fra følgende betragtninger:

(1) Den primære rolle, der varetages af Databeskyttelsesrådet, er at sikre en ensartet anvendelse af GDPR i hele Det Europæiske Økonomiske Samarbejdsområde (**EØS**). I artikel 64, stk. 2, i GDPR hedder det, at en tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen kan kræve, at ethvert almengyldigt spørgsmål eller ethvert spørgsmål, der har virkninger i mere end én EØS-medlemsstat, drøftes af Databeskyttelsesrådet med henblik på en udtalelse.

(2) Databeskyttelsesrådets udtalelse vedtages i henhold til artikel 64, stk. 3, i GDPR sammenholdt med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden senest otte uger efter, at formanden og den kompetente tilsynsmyndighed har besluttet, at sagen er fuldstændig. Efter afgørelse fra formandskabet kan denne frist forlænges med yderligere seks uger under hensyntagen til spørgsmålets kompleksitet –

vedtaget følgende udtalelse:

1 INDLEDNING

1.1 Sammenfatning af de faktiske omstændigheder

1. Den 16. februar 2024 anmodede den franske tilsynsmyndighed Databeskyttelsesrådet om at afgive en udtalelse om foreneligheden med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR af lufthavnsoperatørers og luftfartsselskabers anvendelse af ansigtsgenkendelsesteknologi til biometrisk autentifikation eller identifikation af passagerer[2] med henblik på at strømline passagerstrømmen ved sikkerhedskontrolsteder[3], bagageindlevering, boarding og adgang til passagerloungen i lufthavne (undtagen grænsekontrol og kontrol foretaget af toldfrie butikker) ("**anmodningen**"). Den franske tilsynsmyndighed vedlagde sin anmodning en beskrivelse af typiske brugstilfælde (bilag I).

[1] Henvisninger til "medlemsstater" i denne udtalelse skal forstås som henvisninger til "EØS-medlemsstater". Henvisninger til "Unionen" eller "EU" i hele denne udtalelse skal forstås som henvisninger til "EØS".
[2] I denne udtalelse forstås ved "**passager**" en registreret, hvis personoplysninger behandles til det specifikke formål, der er beskrevet i denne udtalelse. I denne udtalelse anvendes begreberne "passager" og "individ" synonymt.
[3] I denne udtalelse forstås ved "**sikkerhedskontrolsteder i lufthavne**" den sikkerhedskontrol, der udføres under lufthavnsoperatørens ansvar, og som passagererne skal gennemgå for at gå fra afgangshallen til boardingområdet eller boardinggaten.

2. I sin anmodning bemærker den franske tilsynsmyndighed, at de modeller, der i øjeblikket afprøves i flere EU-lufthavne, varierer fra medlemsstat til medlemsstat, og at det kan medføre en risiko for forskelle mellem tilsynsmyndighedernes fortolkninger og en risiko for, at der kan opstå forskellige virkninger for registreredes grundlæggende rettigheder og frihedsrettigheder i EU[4].

3. Databeskyttelsesrådet mener, at følgende spørgsmål skal besvares for at kunne besvare anmodningen fra den franske tilsynsmyndighed:

4. **Spørgsmål 1**:

1.1. Kan brugen af ansigtsgenkendelsesteknologi til biometrisk autentifikation **med det specifikke formål at strømline passagerstrømmen i lufthavne** (sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge) anses for at være forenelig med **artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR** i tilfælde af en lagringsarkitektur, hvor den biometriske skabelon for hver passager alene er lagret **hos den enkelte**, f.eks. lokalt på deres individuelle udstyr, under vedkommendes enekontrol?

1.2. Hvis en sådan behandling anses for at være forenelig med ovennævnte bestemmelser, hvilke fornødne minimumsgarantier vil der da være behov for i lyset af artikel 25 og 32 i GDPR?

Spørgsmål 2:

2.1. Kan brugen af ansigtsgenkendelsesteknologi til biometrisk autentifikation eller identifikation **med det specifikke formål at strømline passagerstrømmen i lufthavne** (sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge) anses for at være forenelig med **artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR** i tilfælde af en **central** lagringsarkitektur, hvor den biometriske skabelon for hver passager er lagret i en central database:

2.1.1. i en central database i lufthavnen under lufthavnsoperatørens kontrol i krypteret form med en nøgle/hemmelighed, der udelukkende opbevares af personen selv (f.eks. på personens mobiltelefon), med henblik på autentifikation?

2.1.2. hvilke fornødne minimumsgarantier vil der være behov for i lyset af artikel 25 og 32 i GDPR, hvis en sådan behandling anses for at være forenelig?

2.2.1. i en central database i lufthavnen under lufthavnsoperatørens kontrol i krypteret form med nøgler, der opbevares af lufthavnsoperatøren, med henblik på identifikation?

2.2.2. hvilke fornødne minimumsgarantier vil der være behov for i lyset af artikel 25 og 32 i GDPR, hvis en sådan behandling anses for at være forenelig?

2.3.1. i skyen under luftfartsselskabets eller dets tjenesteudbyders (databehandlers) kontrol i krypteret form med nøgler, der opbevares af luftfartsselskabet eller dets tjenesteudbyder, med henblik på identifikation?

[4] Anmodningen, s. 1.

2.3.2. hvilke fornødne minimumsgarantier vil der være behov for i lyset af artikel 25 og 32 i GDPR, hvis en sådan behandling anses for at være forenelig?

5. Efter at den franske tilsynsmyndighed den 16. februar 2024 anså sagen for at være fuldstændig, og formanden for Databeskyttelsesrådet den 23. februar 2024 anså sagen for at være fuldstændig, blev sagen videresendt af sekretariatet den 23. februar 2024. Databeskyttelsesrådets formand besluttede i overensstemmelse med artikel 64, stk. 3, i GDPR sammenholdt med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden at forlænge standardfristen for vedtagelse på otte uger med yderligere seks uger på grund af emnets kompleksitet.

1.2 Antagelse til behandling af anmodningen om en udtalelse i henhold til artikel 64, stk. 2, i GDPR

6. I artikel 64, stk. 2, i GDPR fastlægges det, at enhver tilsynsmyndighed kan anmode om, at ethvert spørgsmål, der er almengyldigt eller har virkninger i mere end én medlemsstat, behandles af Databeskyttelsesrådet med henblik på at indhente en udtalelse.

7. Databeskyttelsesrådet mener, at den anmodning, som den franske tilsynsmyndighed har forelagt om foreneligheden af anvendelsen af ansigtsgenkendelsesteknologi til biometrisk autentifikation eller identifikation med det specifikke formål at strømline passagerstrømmen i lufthavne, vedrører spørgsmål, der "har virkninger i mere end én medlemsstat", fordi flere projekter, som forklaret i anmodningen[5], aktuelt er under gennemførelse i medlemsstaternes lufthavne, og det anslås, at en sådan anvendelse vil stige i de kommende år. De modeller, der i øjeblikket afprøves af forskellige lufthavne og luftfartsselskaber, varierer betydeligt fra medlemsstat til medlemsstat, og det kan – ud fra et databeskyttelsesperspektiv – medføre en risiko for, at der opstår divergerende virkninger i mere end én medlemsstat.

8. Databeskyttelsesrådet mener også, at anmodningen fra den franske tilsynsmyndighed har vigtige konsekvenser for anvendelsen af principperne i artikel 5, stk. 1, litra e) og f), i GDPR og de krav, der gælder for dataansvarlige i henhold til artikel 25 i GDPR, samt de krav, der gælder for dataansvarlige og databehandlere i henhold til artikel 32 i GDPR. Denne anmodning vedrører derfor et "almengyldigt spørgsmål" som omhandlet i artikel 64, stk. 2, i GDPR, da den vedrører en konsekvent fortolkning af principperne om lagringsbegrænsning (artikel 5, stk. 1, litra e), i GDPR) og integritet og fortrolighed (artikel 5, stk. 1, litra f), i GDPR) og begreberne databeskyttelse gennem design og databeskyttelse gennem standardindstillinger (artikel 25 i GDPR) og datasikkerhed (artikel 32 i GDPR) for bl.a. at sikre en konsekvent anvendelse af disse bestemmelser i EØS.

9. Eventuelle divergerende holdninger mellem medlemsstaterne til fortolkningen af artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR vil øge risikoen for, at lufthavnsoperatører og luftfartsselskaber udvikler projekter vedrørende ansigtsgenkendelse på en inkonsekvent måde. Da den franske tilsynsmyndighed har påvist, at der er et klart behov for en konsekvent fortolkning af disse bestemmelser i forbindelse med ansigtsgenkendelsesteknologi til biometrisk autentifikation eller identifikation af passagerer for at strømline passagerstrømmen i lufthavne[6], mener Databeskyttelsesrådet, at anmodningen er begrundet i overensstemmelse med artikel 10, stk. 3, i Databeskyttelsesrådets forretningsorden.

[5] Anmodningen, s. 3.
[6] Anmodningen, s. 1.

10. I henhold til databeskyttelsesforordningens artikel 64, stk. 3, afgiver Databeskyttelsesrådet ikke en udtalelse, hvis det allerede har afgivet en udtalelse om samme spørgsmål[7]. Databeskyttelsesrådet har endnu ikke besvaret de spørgsmål, der er opstået som følge af anmodningen. Selv om Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger[8] allerede indeholder nogle nyttige elementer om de sikkerhedsforanstaltninger, der bør anvendes i forbindelse med behandling af biometriske data, behandler de ikke alle aspekter vedrørende de spørgsmål, der rejses i anmodningen. Databeskyttelsesrådets tilgængelige vejledning, herunder Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, giver ikke specifik vejledning om mulige elementer, der skal verificeres i forbindelse med central eller decentral lagring af biometriske data med henblik på at identificere eller autentificere passagerer for at strømline passagerstrømmen i lufthavne, eller om foreneligheden af en sådan behandling med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR.

11. Af disse grunde mener Databeskyttelsesrådet, at anmodningen kan antages, og at de spørgsmål, der rejses deri, bør analyseres i en udtalelse, der vedtages i henhold til databeskyttelsesforordningens artikel 64, stk. 2.

2 UDTALELSENS ANVENDELSESOMRÅDE OG SAMMENHÆNG

2.1 Udtalelsens anvendelsesområde

12. Denne udtalelse vedrører kun foreneligheden med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR af lufthavnsoperatørers og luftfartsselskabers anvendelse af ansigtsgenkendelsesteknologi til biometrisk autentifikation eller identifikation af passagerer **med det specifikke formål at strømline passagerstrømmen i lufthavne**, dvs. ved sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge, som det fremgår af anmodningen.

13. Med hensyn til **anvendelsesområdet for denne udtalelse** præciserer Databeskyttelsesrådet følgende:

    1) Behandling af personoplysninger i forbindelse med grænsekontrol og kontrol foretaget af toldfrie butikker er ikke omfattet af denne udtalelse, da de udføres af andre dataansvarlige end lufthavnsoperatører og luftfartsselskaber.

    2) Anvendelsen af ansigtsgenkendelsesteknologi, selv når den er baseret på de scenarier, der er beskrevet nedenfor i afsnit 3.2, til andre formål (f.eks. retshåndhævelse) eller af andre parter, selv om det sker til lignende formål, er ikke omfattet af denne udtalelse.

    3) I denne udtalelse undersøges kun behandlingen af passagerers personoplysninger, og udtalelsen omfatter ikke andre typer registrerede som f.eks. lufthavnsoperatørers eller luftfartsselskabers personale.

    4) I denne udtalelse undersøges anmodningen som indgivet af den franske tilsynsmyndighed med hensyn til foreneligheden af lagringsarkitekturen i passagerernes biometriske skabeloner med artikel 5, stk. 1, litra e) og f), samt artikel

[7] Artikel 64, stk. 3, i GDPR og artikel 10, stk. 4, i Databeskyttelsesrådets forretningsorden.
[8] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger, version 2.0, vedtaget den 29.1.2020 ("**Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr**").

25 og 32 i GDPR. I denne henseende indeholder denne udtalelse ikke en fuldstændig analyse af de relevante dataansvarliges og deres eventuelle databehandleres overholdelse af GDPR i hvert enkelt tilfælde. Dette er særlig vigtigt i betragtning af, at disse teknologier indebærer øgede risici i forbindelse med behandlingen af de særlige kategorier af oplysninger i overensstemmelse med artikel 9 i GDPR. Denne udtalelse berører derfor ikke en vurdering af andre bestemmelser i GDPR, når det drejer sig om anvendelsen af ansigtsgenkendelsesteknologier, herunder i den specifikke sektor, som anmodningen vedrører, eller en juridisk og teknisk analyse fra sag til sag baseret på en dataansvarligs specifikke påtænkte behandling og omstændigheder.

5) Denne udtalelse undersøger ikke behandlingen af børns personoplysninger og berører ikke eventuelle specifikke krav, der gælder i denne henseende.

6) Denne udtalelse berører ikke retlige krav og yderligere begrænsninger for anvendelsen af biometriske data, der følger af medlemsstaternes nationale lovgivning[9].

7) Enhver konklusion i denne udtalelse berører ikke yderligere teknologisk udvikling.

8) I denne udtalelse undersøges fire scenarier, hvis specifikke karakteristika er beskrevet nedenfor i afsnit 3.2. Udtalelsen omhandler ikke andre scenarier, selv om behandlingen foretages til de samme formål.

14. I sin anmodning anførte den franske tilsynsmyndighed, at behandlingen af passagerernes biometriske data med henblik på at strømline passagerstrømmen i lufthavne ville være baseret på den antagelse, at de pågældende personer giver samtykke til en sådan behandling, hvilket muligvis ville udgøre retsgrundlaget i henhold til GDPR[10]. **Analysen af det gældende retsgrundlag er desuden ikke omfattet af de spørgsmål, der er forelagt Databeskyttelsesrådet i anmodningen, og som følge heraf undersøges gyldigheden af samtykke til en sådan behandling i overensstemmelse med artikel 6, 7 og 9 i GDPR ikke i denne udtalelse.**

15. Databeskyttelsesrådet bemærker imidlertid generelt, at de relevante dataansvarlige, hvis de vil basere sig på dette retsgrundlag, skal indhente et gyldigt udtrykkeligt samtykke[11] fra personer, der er villige til at bruge sådanne tjenester. Et sådant udtrykkeligt samtykke skal gives frivilligt, specifikt og informeret[12], og det analyseres fra sag til sag, om disse betingelser er opfyldt. Dette bl.a. betyder, at:

1) Personer skal til enhver tid let kunne trække et sådant samtykke tilbage, uden at de udsættes for ulemper[13].

---

[9] F.eks. fastsættes det i artikel 9, stk. 4, i GDPR, at medlemsstaterne kan opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af biometriske data.

[10] Anmodningen, bilag I.

[11] I henhold til artikel 4, nr. 14), samt artikel 9, stk. 1, og artikel 9, stk. 2, litra a), i GDPR er behandling af biometriske data med det formål entydigt at identificere en fysisk person forbudt, medmindre den registrerede har givet udtrykkeligt samtykke til behandling af disse personoplysninger til et eller flere specifikke formål, undtagen hvor EU-retten eller medlemsstaternes nationale ret fastsætter, at forbuddet i artikel 9, stk. 1, i GDPR ikke kan ophæves af den registrerede. Se også betragtning 51, 52 og 53 til GDPR.

[12] Artikel 4, nr. 11), og artikel 7 i GDPR.

[13] Artikel 7, stk. 4, i GDPR, og betragtning 50 til GDPR.

2) For at samtykke kan anses for at være givet frivilligt, kan en sådan anvendelse af biometriske teknologier kun finde sted på frivillig basis, da personer frit bør kunne vælge, om de vil bruge disse tjenester eller ej, og uden at de udsættes for ulemper (f.eks. betydeligt længere forsinkelser for passagerer, der ikke giver samtykke[14]), incitamenter, yderligere omkostninger eller yderligere fordele til gengæld[15].

3) Der skal også indhentes udtrykkeligt samtykke fra personer, hvis biometriske data behandles, selv om de ikke har registreret sig med henblik på at blive identificeret eller autentificeret ved hjælp af sådanne midler. Det er med andre ord vigtigt, at personer, der ikke udtrykkeligt har givet samtykke til ansigtsgenkendelse til det tilsigtede formål, ikke får deres ansigter scannet af kameraer. Dette kan f.eks. opnås ved at afsætte specifikke baner til ansigtsgenkendelse og sørge for passende skiltning og fysisk adskillelse med de ikkebiometriske kontrolstrømme for at muliggøre en klar identifikation af sådanne baner.

4) Uden at det berører spørgsmålet om, hvorvidt samtykke vil være det gældende retsgrundlag for en sådan behandling, finder principperne om behandling, der er fastsat i artikel 5 i GDPR med hensyn til nødvendighed og proportionalitet, stadig anvendelse, selv når personer har givet deres udtrykkelige samtykke til anvendelsen af deres biometriske data[16].

16. Ifølge anmodningen[17] vil lufthavnsoperatørerne fungere som dataansvarlige ved behandlingen på sikkerhedskontrolsteder i lufthavne, mens luftfartsselskaberne vil fungere som dataansvarlige ved behandlingen ved bagageindlevering, boarding og adgang til passagerloungen. Databeskyttelsesrådet bemærker derfor, at forskellige aktører kan være involveret i den behandling, der er beskrevet i anmodningen, og det har ikke vurderet anvendelsen af rollerne som (fælles) dataansvarlig og/eller databehandler i de scenarier, der er beskrevet nedenfor i afsnit 3.2 i denne udtalelse. I hvert enkelt tilfælde skal de involverede aktører identificeres, og deres ansvar skal fordeles klart, så kravene i GDPR er opfyldt[18].

17. Databeskyttelsesrådet bemærker endvidere, at der i øjeblikket ikke er et ensartet lovkrav i EU om, at lufthavnsoperatører og luftfartsselskaber skal identificere passagerer og verificere, at navnet på passagerens boardingkort svarer til navnet på deres identitetsdokument, på alle ovennævnte

[14] Dette kan f.eks. omfatte overvejelser med det formål at udforme system, som undgår at skabe socialt pres på passagerer, der ikke ønsker at give deres samtykke, ved at undgå, at deres valg påvirker andre passagerer negativt.

[15] Databeskyttelsesrådets retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4.5.2020 (**Databeskyttelsesrådets retningslinjer 5/2020 vedrørende samtykke**), punkt 46 og 48).

[16] Idem., punkt 5.

[17] Anmodningen, bilag I.

[18] I overensstemmelse med artikel 4, stk. 7 og 8, artikel 5, stk. 2, samt artikel 24, 26, 28 og 29 i GDPR. Se også Databeskyttelsesrådets retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse, version 2,1, vedtaget den 7.7.2021

kontrolsteder[19]. Sådanne krav er således underlagt national lovgivning, der kan variere fra medlemsstat til medlemsstat. I nogle medlemsstater kan en sådan kontrol være påkrævet for nogle kontrolsteder (f.eks. bagageindlevering eller boarding), mens en sådan kontrol på nuværende tidspunkt ikke er påkrævet i andre[20]. Tilstedeværelsen af juridiske forpligtelser til at kontrollere passagerernes identitet har en direkte indvirkning på de forskellige lufthavnes praksis.

18. I disse situationer, **hvor der ikke kræves verifikation af passagerernes identitet med et officielt identitetsdokument, bør der ikke foretages verifikation ved hjælp af biometrisk teknologi, da dette vil føre til en overdreven behandling af oplysninger, da det indebærer behandling af yderligere oplysninger i forhold til den nuværende situation og vil gå ud over, hvad der er nødvendigt til det relevante formål, i strid med princippet om dataminimering i artikel 5, stk. 1, litra c), i GDPR.** Et sådant hensyn skal tages i betragtning i forbindelse med undersøgelsen af alle de scenarier, der er beskrevet nedenfor i afsnit 3.2 i denne udtalelse.

2.2 Centrale begreber

19. For at dataene skal kunne betragtes som biometriske data i henhold til artikel 4, nr. 14), i GDPR[21] skal behandlingen af rådata såsom fysiske, fysiologiske eller adfærdsmæssige karakteristika for en fysisk person indebære en måling af disse karakteristika, da biometriske data er resultatet af sådanne målinger[22].

20. Ved at bruge billedet af en persons ansigt (et fotografi eller en video), som kaldes en biometrisk "**prøve**", er det muligt at udtrække en digital repræsentation af forskellige karakteristika for dette ansigt (dette kaldes en "**skabelon**")[23]. Databeskyttelsesrådet minder desuden om, at en "biometrisk skabelon er en digital repræsentation af de entydige træk fra en biometrisk prøve, og den kan gemmes i en biometrisk database"[24], som muliggør eller bekræfter entydig identifikation af en fysisk person. Denne "skabelon formodes at være entydig og specifik for hver person, og den kan i princippet ikke ændres med tiden"[25]. I en sammenligningsproces, der har til formål at identificere eller autentificere

[19] Den relevante forordning på EU-plan er Kommissionens gennemførelsesforordning (EU) 2015/1998 af 5. november 2015 om detaljerede foranstaltninger til gennemførelse af de fælles grundlæggende normer for luftfartssikkerhed. Denne forordning omhandler imidlertid ikke kontrol af officielle identitetsdokumenter på kontrolsteder i lufthavne, og medlemsstaterne har beføjelse til at regulere dette på nationalt plan.
[20] Det betyder, at der i øjeblikket enten slet ikke foretages nogen verifikation, eller at kun boardingkortets eksistens kontrolleres. På grundlag af protokollen af 22.5.1954 vedrørende fritagelse for statsborgere i Danmark, Finland, Norge og Sverige for at være i besiddelse af pas og opholdstilladelse under ophold i andet nordisk land end hjemlandet er statsborgere i Norge, Danmark, Finland og Sverige fra den 1.7.1954 fritaget for forpligtelsen til at være i besiddelse af pas eller anden rejselegitimation, når de rejser mellem disse lande.
[21] Se også betragtning 51, 52 og 53 til GDPR.
[22] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 74.
[23] Databeskyttelsesrådets retningslinjer 05/2022 om brug af ansigtsgenkendelsesteknologi inden for retshåndhævelse, version 2.0, vedtaget den 26. april 2023 (**Databeskyttelsesrådets retningslinjer 5/2022 for anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet**), punkt 7 og 8.
[24] Idem., punkt 9.
[25] Idem.

en person via ansigtsgenkendelse, sammenlignes en modtaget biometrisk skabelon typisk med objekter, der er lagret, for at verificere et match eller finde et match i en database[26].

21. Ansigtsgenkendelsesteknologi kan opfylde to forskellige funktioner – autentifikation[27] og identifikation[28]. Selv om de to funktioner er forskellige, er de begge afhængige af behandling af biometriske data vedrørende en identificeret eller identificerbar fysisk person[29] og udgør derfor behandling af særlige kategorier af personoplysninger i henhold til artikel 9 i GDPR[30].

22. Navnlig gælder følgende:

> **Autentifikation** har til formål at bekræfte en biometrisk påstand gennem sammenligning. Dette kaldes også 1:1-verifikation.
>
> **Identifikation** har til formål at søge i en database med biometriske registreringer for at returnere identifikatorer, der kan tilskrives en enkelt person. Dette kaldes også 1:mange-identifikation.

23. I begge tilfælde er de anvendte ansigtsgenkendelsesteknikker baseret på et estimeret match mellem skabeloner, den, der sammenlignes, og en eller flere baselines. Fra dette synspunkt er processen probabilistisk: Sammenligningen bestemmer en højere eller lavere sandsynlighed for, at personen faktisk er den person, der skal autentificeres eller identificeres. Hvis denne sandsynlighed overstiger en vis tærskel i systemet, defineret af brugeren eller udvikleren af systemet, vil systemet antage, at der er et match, som skal identificeres eller autentificeres[31].

---

[26] Databeskyttelsesrådets retningslinjer 5/2022 om ansigtsgenkendelse i forbindelse med retshåndhævelse, punkt 10-11. Se også den internationale standard ISO/IEC 2382-37, 2022-03, som findes på: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [tilgået den 23.5.2024] ("**ISO/IEC 2382-37**").

[27] Databeskyttelsesrådet bemærker, at Europa-Parlamentets og Rådets kommende forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) (endnu ikke offentliggjort i EUT) i artikel 3, nr. 36), også definerer "biometrisk verifikation" som "automatisk, en-til-en-verifikation, herunder autentificering, af fysiske personers identitet ved at sammenligne deres biometriske data med tidligere afgivne biometriske data" (se Europa-Parlamentets lovgivningsmæssige beslutning af 13. marts 2024 om forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter (COM(2021) 0206 – C9-0146/2021 – 2021/0106(COD)).

[28] Idem., artikel 3, nr. 35), i forordningen om kunstig intelligens definerer "biometrisk identifikation" som "automatisk genkendelse af fysiske, fysiologiske, adfærdsmæssige eller psykologiske menneskelige træk med henblik på at fastslå en fysisk persons identitet ved at sammenligne den pågældende persons biometriske data med biometriske data om enkeltpersoner lagret i en database".

[29] ISO/IEC 2382-37.

[30] Artikel 4, nr. 14), i GDPR og Databeskyttelsesrådets retningslinjer 5/2022 om ansigtsgenkendelse i forbindelse med retshåndhævelse, punkt 12.

[31] Databeskyttelsesrådets retningslinjer 5/2022 om ansigtsgenkendelse i forbindelse med retshåndhævelse, punkt 11. Se også ISO/IEC 2382-37.

3 SPØRGSMÅLET OM ANMODNINGENS BERETTIGELSE

3.1 Almindelige bemærkninger

24. I dette afsnit analyseres spørgsmålene i punkt 4 ovenfor. I denne forbindelse vil Databeskyttelsesrådet for så vidt angår spørgsmål 1 analysere foreneligheden med artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR og for så vidt angår spørgsmål 2 foreneligheden med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR.

25. Med henblik herpå vil Databeskyttelsesrådet analysere fire forskellige scenarier[32], hvis specifikke karakteristika er beskrevet nedenfor i afsnit 3.2.

26. Indledningsvis minder Databeskyttelsesrådet om, at anvendelsen af biometriske data og navnlig ansigtsgenkendelsesteknologi indebærer øgede risici for de registreredes rettigheder og frihedsrettigheder. For det første vedrører den pågældende behandling biometriske data, som er omfattet af særlig beskyttelse i henhold til artikel 9 i GDPR. Biometriske data ændrer uigenkaldeligt forholdet mellem krop og identitet, idet oplysningerne gør den menneskelige krops karakteristika "maskinaflæselige" og giver mulighed for yderligere anvendelse[33]. Brugen af ansigtsgenkendelsesteknologi kan desuden føre til risici forbundet med falske negativer, forudindtagethed og forskelsbehandling[34], og potentielt misbrug af biometriske data kan have alvorlige konsekvenser for enkeltpersoner, f.eks. identitetssvig eller imitation[35]. Når ansigtsgenkendelse foretages på afstand og uden aktiv inddragelse af den registrerede, skal det bemærkes, at de pågældende personer kan være endnu mindre opmærksomme på en sådan behandling og de dermed forbundne risici. Endelig er det vigtigt at understrege, at de karakteristika, som biometriske data er baseret på, generelt kan betragtes som permanente og bør behandles som uigenkaldelige, navnlig i forbindelse med ansigtsgenkendelse[36].

27. Under hensyntagen til ovenstående bør de dataansvarlige, inden sådanne teknologier anvendes, og selv om teknologierne anses for at være særligt effektive, vurdere indvirkningen på de registreredes

---

[32] De fire scenarier, som Databeskyttelsesrådet har analyseret, er baseret på de brugstilfælde, der er beskrevet i bilag I til anmodningen. Den franske tilsynsmyndighed har præciseret, at de brugstilfælde, der er anført i bilag I til anmodningen, er eksempler på gennemførelse, der tilhører et scenarie, og som anvendes til illustrative formål.

[33] Artikel 29-Gruppens udtalelse 3/2012 om udviklingen inden for biometriske teknologier vedtaget den 27.4.2012, WP193 ("**Artikel 29-Gruppens udtalelse 3/2012 om biometriske teknologier**"), s. 4. Det skal bemærkes, at denne udtalelse henviser til direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ("databeskyttelsesdirektivet"). GDPR har udvidet anvendelsesområdet for de særlige kategorier af oplysninger, og i modsætning til databeskyttelsesdirektivet fastsættes det i GDPR, at biometriske data er særlige kategorier af oplysninger (artikel 9 i GDPR).

[34] Guidelines on facial recognition, Europarådets rådgivende udvalg om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, juni 2021, s. 15. Se også Databeskyttelsesrådets retningslinjer 5/2022 om ansigtsgenkendelse i forbindelse med retshåndhævelse, punkt 27.

[35] Artikel 29-Gruppens udtalelse 3/2012 om biometriske teknologier, s. 29.

[36] Databeskyttelsesrådets retningslinjer 5/2022 om ansigtsgenkendelse i forbindelse med retshåndhævelse, punkt 104.

grundlæggende rettigheder og frihedsrettigheder og overveje, om mindre indgribende midler kan opfylde deres legitime formål med behandlingen[37].

28. Databeskyttelsesrådet minder også om, at retten til beskyttelse af personoplysninger ikke er en absolut ret; den skal afvejes i forhold til andre grundlæggende rettigheder, der er beskyttet af chartret, i overensstemmelse med proportionalitetsprincippet[38].

29. Artikel 25, stk. 1, i GDPR henviser til de "databeskyttelsesprincipper", der er anført i artikel 5 i GDPR[39], og kræver, at de "er designet med henblik på effektiv implementering"[40]. Dette omfatter udtrykkeligt princippet om dataminimering i henhold til artikel 5, stk. 1, litra c), i GDPR[41], som kræver, at personoplysninger er "tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles, jf. proportionalitetsprincippet"[42]. Desuden præciseres forpligtelsen til "dataminimering gennem standardindstillinger" i artikel 25, stk. 2, i GDPR, idet det angives, at forpligtelsen gælder mængden af indsamlede personoplysninger og omfanget af deres behandling, opbevaringsperiode og tilgængelighed[43].

30. I henhold til artikel 25 i GDPR skal dataansvarlige imidlertid ikke gennemføre specifikke tekniske og organisatoriske foranstaltninger. De skal derimod sikre, at de valgte foranstaltninger og garantier er specifikke for sammenhængen risiciene for den registreredes rettigheder og frihedsrettigheder som følge af behandlingen[44]. Tilsvarende kræves det i artikel 32 i GDPR om behandlingssikkerhed, at dataansvarlige og databehandlere gennemfører passende tekniske og organisatoriske

---

[37] Betragtning 39 til GDPR. Se også Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 73.

[38] Betragtning 4 til GDPR. Se i denne forbindelse også Domstolens dom af 22.6.2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 ("C-439/19 Latvijas Republikas Saeima"), præmis 98, 110 og 113. Endvidere kræver proportionalitetsprincippet som et generelt princip i EU-retten, at de foranstaltninger, som iværksættes ved EU-retsakter, er egnede til at nå det tilstræbte mål og ikke går ud over, hvad der er nødvendigt for at nå det (se Domstolens dom af 9.11.2010, Volker und Markus Schecke og Eifert, C-92/09 og C-93/09, ECLI:EU:C:2010:662 ("C-92/09 og C-93/09 Volker und Schecke"), præmis 74 og den deri nævnte retspraksis).

[39] Databeskyttelsesrådets retningslinjer 4/2019 om Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i henhold til artikel 25, version 2.0, vedtaget den 20.10.2020 ("**Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger**", punkt 11).

[40] Artikel 25, stk. 1, i GDPR lyder: "Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder". Se også Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25, punkt 13.

[41] Tilsvarende anføres det i betragtning 39 til GDPR, at personoplysninger kun bør behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde.

[42] C-439/19 Latvijas Republikas Saeima, præmis 98, Domstolens dom af 11.12. 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 ("C-708/18 M5A-ScaraA"), præmis 48.

[43] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25, punkt 48.

[44] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25, punkt 14.

foranstaltninger for at sikre et sikkerhedsniveau, der passer til risikoen for fysiske personers rettigheder og frihedsrettigheder.

31. Det er vigtigt at bemærke, at principperne for behandling af personoplysninger i GDPR vedrørende nødvendighed og proportionalitet finder anvendelse og skal overholdes, selv om passagererne udtrykkeligt giver samtykke til, at deres biometriske data anvendes til at strømline passagerstrømmen i lufthavne[45].

32. Med hensyn til **nødvendighedsprincippet** vil Databeskyttelsesrådet overveje, om den foreslåede behandling er nødvendig for at nå det omhandlede mål, og om det samme mål kan nås lige så godt på en anden måde, som er mindre indgribende i de berørte personers grundlæggende rettigheder og frihedsrettigheder[46]. Med hensyn til **proportionalitetsprincippet** vil Databeskyttelsesrådet vurdere, om den negative indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder står i et rimeligt forhold til eventuelle forventede fordele. Hvis fordelen er relativt lille, er en sådan virkning muligvis ikke proportional[47].

33. Selv om Databeskyttelsesrådet mener, at et af de scenarier, der analyseres nedenfor, opfylder kravene i artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR, er det under alle omstændigheder, den dataansvarlige, der i hvert enkelt tilfælde skal påvise dette med faktuelle oplysninger. En sådan påvisning bør omfatte overvejelser om alternative scenarier.

3.2 Om foreneligheden med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR

3.2.1 Scenarie 1: opbevaring af registrerede biometriske skabeloner udelukkende hos den enkelte med henblik på autentifikation

34. I dette afsnit undersøges det, om det er foreneligt med artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR, når passagerernes biometriske skabelon kun opbevares hos den enkelte, f.eks. på vedkommendes individuelle enhed[48], under dennes enekontrol[49], med henblik på autentifikation[50] ("**scenarie 1**"). I dette afsnit undersøges også de fornødne garantier for scenarie 1 i lyset af artikel 25 og 32 i GDPR.

Beskrivelse af scenariet

35. I scenarie 1 lagres den registrerede biometriske skabelon for hver passager, der har givet samtykke til en sådan behandling, kun hos den enkelte person, f.eks. på en individuel enhed, som hver passager opbevarer under dennes enekontrol. Passagererne verificeres (1:1-sammenligning), når de passerer specifikke kontrolsteder i lufthavnen.

---

[45] Databeskyttelsesrådets retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, punkt 5.
[46] C-439/19 Latvijas Republikas Saeima, præmis 110 og 113, og Domstolens dom (Store Afdeling) af 4.7.2023, Meta mod Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, præmis 108.
[47] C-708/18 M5A-ScaraA, præmis 52-56, C-92/09 og C-93/09 Volker og Schecke, præmis 87, og C-439/19 Latvijas Republikas Saeima, præmis 98, 110 og 113. Se også Artikel 29-Gruppens udtalelse 3/2012 om biometriske teknologier, s. 8.
[48] Alternativt kan personen udskrive og opbevare sin biometriske skabelon på papir.
[49] Dette berører ikke den dataansvarliges overordnede ansvar for behandlingen.
[50] Som vist ved brugstilfælde 1 i bilag I til anmodningen.

36. Registreringen foretages af lufthavnsoperatøren, enten via lufthavnsoperatørens app[51] eller i lufthavnsterminaler med et passende identitetssikringsniveau (f.eks. eIDAS-sikkerhedsniveau[52]). En sådan registrering består i at registrere en biometrisk skabelon og de identifikationsoplysninger, der er nødvendige for behandlingen, på passagerens enhed[53] ("**ID**"). Registreringen sker kun én gang og for en bestemt gyldighedsperiode (f.eks. i overensstemmelse med gyldighedsperioden for passagerernes pas). Hverken passagerernes ID eller deres biometriske data opbevares af lufthavnsoperatøren efter registreringsprocessen.

37. Navnlig med hensyn til lagring gemmes passagerens ID og biometriske skabelon lokalt på hver passagers enhed (f.eks. lufthavnsoperatørens mobilapp eller i en digital tegnebogsapp). Enheden kan derefter bruges til at overføre eller søge i passagerernes ID og biometriske skabelon, eventuelt med flyoplysninger og/eller boardingkortet. Disse oplysninger krypteres f.eks. med en nøgle, som opbevares af lufthavnsoperatøren alene – eventuelt kodet i form af en QR-kode, som enten kan udskrives på papir eller vises på skærmen på passagerens enhed. I dette tilfælde vil passageren derefter fremvise denne QR-kode på særlige kontrolstandere ("pods") i lufthavnen, som er udstyret med en QR-scanner og et kamera.

38. Med hensyn til sikkerhed dekrypteres QR-koder under matchningen med en nøgle, der opbevares af lufthavnsoperatøren, som er den eneste, der kan dekryptere QR-koderne. Passagerernes biometriske data opbevares kun i en meget kort periode og slettes, når matchningen er afsluttet. Det skal bemærkes, at sikkerhedsforanstaltningerne vedrørende opbevaring delvis afhænger af passagerenhedens sikkerhed.

Databeskyttelsesrådets vurdering

39. Scenarie 1 beskriver tekniske og organisatoriske foranstaltninger, der er udformet med henblik på at sikre et sikkerhedsniveau, der står i et rimeligt forhold til risiciene for de registrerede, som det kræves i artikel 5, stk. 1, litra f), og artikel 32 i GDPR. Passagererne verificeres (1:1-sammenligning), når de passerer specifikke kontrolsteder i lufthavnen. I dette scenarie foretages den vigtigste matchning i et kontrolleret miljø[54], hvor passagererne er aktivt involveret og har mere kontrol over deres data. Kun passagerer, der har givet samtykke til en sådan behandling, vil blive kontrolleret, og der vil ikke blive indsamlet biometriske data om andre passagerer, som ikke har givet samtykke til en sådan behandling, da kontrollen sker ved særlige standere. De passagerer, der har givet samtykke, kan desuden til enhver tid mulighed for at stoppe behandlingen ved at slette dataene fra deres enhed.

[51] Databeskyttelsesrådet bemærker, at der i fremtiden kan overvejes alternative registreringsmåder, og at registreringen muligvis kan foretages uden en bestemt lufthavnsoperatørs app, f.eks. ved hjælp af interaktion med en brugers digitale tegnebog.

[52] En ramme for elektronisk identifikation og tillidstjenester ("**eIDAS**") baseret på Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet.

[53] I denne udtalelse forstås ved identifikationsoplysninger oplysninger som f.eks. efternavn, fornavn, fødselsdato osv., som er blevet verificeret som korrekte i forhold til et identitetsdokument eller pas.

[54] "Ukontrolleret miljø" henviser til anvendelse af ansigtsgenkendelse til identifikation uden aktiv inddragelse af de registrerede, hvor skabelonen for hvert ansigt, der kommer ind i overvågningsområdet, sammenlignes med skabeloner fra et bredt tværsnit af den population, der er lagret i en database (se Databeskyttelsesrådets retningslinjer 5/2022 om ansigtsgenkendelse i forbindelse med retshåndhævelse, punkt 17).

40. Anvendelsen af ansigtsgenkendelse baseret på en biometrisk skabelon, der kun er lagret hos den enkelte, og som f.eks. kan være på en individuel enhed, som passageren har enekontrol over, og som anvendes til autentifikation ved specifikke kontrolsteder via en særlig grænseflade, indebærer under visse omstændigheder færre risici sammenlignet med anvendelsen af biometriske data, hvor dataene er lagret i en central database[55]. En sådan lokal opbevaring mindsker, når den ledsages af de fornødne garantier[56], alvoren af brud på persondatasikkerheden sammenlignet med central lagring, når det drejer sig om antallet af berørte personer, og sikrer, at adgangen til den biometriske skabelon indebærer en aktiv inddragelse af den registrerede.

41. Matchningen kan desuden foretages lokalt i lufthavnen ved at sammenligne den biometriske skabelon, f.eks. indeholdt i QR-koden, med resultatet af skabelonen beregnet på grundlag af den biometriske prøve, der er optaget af kameraet på en kontrolstander. Kun det matchende resultat vil blive meddelt og anvendt af den dataansvarlige, der udfører en specifik kontrol (som kan være enten en lufthavnsoperatør eller et luftfartsselskab afhængigt af, om det sker ved sikkerhedskontrol, bagageindlevering, boarding eller adgang til passagerloungen i lufthavnen). Det forhold, at de oplysninger, der kræves til matchningen (f.eks. QR-koden), skal gives af personen, fungerer som en anden faktor[57] og styrker dermed sikkerheden i forbindelse med autentifikationen.

42. Med hensyn til foreneligheden med artikel 25 i GDPR og navnlig for at opfylde kravet om dataminimering bør det sikres, at behandlingen opfylder nødvendighedsprincippet. I scenarie 1 kan de valgte foranstaltninger anses for at have opfyldt nødvendighedsprincippet i forhold til det omhandlede mål (dvs. strømlining af passagerstrømmen), hvis den dataansvarlige – afhængigt af omstændighederne – kan påvise, at der ikke findes mindre indgribende alternative løsninger, der kan nå det samme mål lige så effektivt. Den dataansvarlige kan f.eks. påvise, at scenarie 1 – selv hvis passagererne skulle fremvise deres enhed – fremskynder verifikationsprocessen i forhold til den nuværende situation, som omfatter en menneskelig kontrol af, om navnet på boardingkortet stemmer overens med passagerens identitetsdokument[58]. Dette kan navnlig ikke påvises, hvis der i øjeblikket ikke foretages kontrol for at verificere passagerernes identitet på grundlag af deres officielle identitetsdokument (se i denne henseende punkt 18 ovenfor).

43. Lufthavnsoperatøren opbevarer endvidere ikke biometriske skabeloner efter registreringen, og opbevaringsperioden for de biometriske data hos den dataansvarlige, der foretager kontrollen, er meget kort, da sådanne oplysninger slettes, så snart matchningen er afsluttet. De foranstaltninger, der er valgt i scenarie 1, synes således at begrænse omfanget af behandlingen og opbevaringsperioden for personoplysningerne.

44. Med hensyn til proportionalitetsprincippet kan den indgribende karakter af en sådan behandling opvejes af passagerernes aktive inddragelse, da deres biometriske data kun vil blive lagret hos dem selv. Under hensyntagen til de ovenfor beskrevne foranstaltninger og under forudsætning af, at den dataansvarlige gennemfører de fornødne garantier som krævet i forbindelse med den pågældende specifikke behandling, kan gennemførelsen af passende foranstaltninger desuden sikre et

[55] Databeskyttelsesrådets retningslinjer 5/2022 om ansigtsgenkendelse i forbindelse med retshåndhævelse, punkt 17.
[56] Som nævnt nedenfor i punkt 46.
[57] Dette mindsker f.eks. risikoen for identitetsspoofing. Se også garanti C.1.2 nedenfor.
[58] Det kan også hævdes, at den biometriske kontrol kan gives anledning til færre fejl end en menneskelig kontrol.

sikkerhedsniveau, der er i overensstemmelse med risikoen. I så fald kan den negative indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder anses for at stå i et rimeligt forhold til den forventede fordel.

45. I betragtning af ovenstående konkluderer Databeskyttelsesrådet derfor som svar på spørgsmål 1.1, at en sådan behandling **i princippet kan anses for at være forenelig med artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR med forbehold af de fornødne garantier**.

Fornødne garantier

46. I denne type scenarie mener Databeskyttelsesrådet som svar på spørgsmål 1.2, at der som minimum bør gennemføres følgende garantier. Andre garantier end dem, der er beskrevet i denne udtalelse, kan anvendes til at nå de samme sikkerheds- og databeskyttelsesmål og kan være lovlige, så længe de sikrer overholdelse af den gældende retlige ramme.

47. Bemærk: Dette er en overordnet og ikke-udtømmende oversigt over de mulige fornødne garantier, som bør gennemføres af en dataansvarlig i en løsning svarende til scenarie 1. Hvorvidt de er hensigtsmæssige i henhold til artikel 25 og 32 i GDPR, afhænger af en konkret vurdering fra sag til sag. Alle dataansvarlige skal sikre, at de foretager deres egen konsekvensanalyse vedrørende databeskyttelse[59]. Deres specifikke løsninger kan kræve yderligere foranstaltninger, som ikke er medtaget i denne udtalelse.

A. Generelle spørgsmål

A.1 Konsekvensanalyse vedrørende databehandling

A.1.1 Foretag en konsekvensanalyse vedrørende databeskyttelse i overensstemmelse med kravene i artikel 35 i GDPR, når den dataansvarlige planlægger en ny behandlingsaktivitet, der sandsynligvis vil medføre en høj risiko. Dette vil sandsynligvis være tilfældet med scenarie 1, da det indebærer behandling af biometriske data i stor skala[60]. Vurder hensigtsmæssigheden af at indføre et ansigtsgenkendelsessystem, herunder om det er nødvendigt og står i rimeligt forhold til formålene[61], i den tidlige designfase, og gennemgå det i hele produktudviklingens livscyklus.

A.1.2 Konsulter den relevante tilsynsmyndighed, hvis behandlingen stadig medfører en høj risiko på trods af de foranstaltninger, som den dataansvarlige har truffet for at mindske risikoen[62].

A.2 Registreredes rettigheder og garantier, der kan gennemføres af dataansvarlige

[59] Artikel 35 i GDPR.
[60] Artikel 35, stk. 3, GDPR og Artikel 29-Gruppen vedrørende Databeskyttelse: Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, vedtaget den 13.10.2017, WP248rev.01, godkendt af Databeskyttelsesrådet.
[61] Artikel 35, stk. 7, litra b), i GDPR.
[62] Artikel 36, stk. 1, i GDPR.

A.2.1 Garantier til håndtering af tilfælde af falsk negativ. Begræns risikoen for alders-, køns- og racemæssige skævheder ved regelmæssigt at "vurdere, om algoritmerne virker i overensstemmelse med formålene, og tilpasse algoritmerne, så de afbøder systemiske fejl og sikrer rimelighed i behandlingen"[63], f.eks. ved at gennemføre menneskeligt tilsyn og indgriben for at afbøde eventuelle skævheder og sikre, at der ikke sker stigmatisering eller profilering af passagerer.

A.2.2 Sørg for, at al behandling af personoplysninger er gennemsigtig, og at personer er opmærksomme på og har kontrol over, hvordan deres oplysninger behandles for hver behandlingsaktivitet[64].

A.2.3 Sørg for, at der er truffet foranstaltninger til at overholde princippet om formålsbegrænsning, så oplysningerne ikke anvendes til andre formål, f.eks. til sikkerheds- eller uddannelsesformål.

A.2.4 Sørg for, at der ikke tages billeder eller optages video af personer, der ikke giver samtykke til ansigtsgenkendelse, ved hjælp af passende foranstaltninger (f.eks. ved at anvende en tilstrækkelig dybdeskarphed og et tilstrækkeligt optagelsesområde for at undgå at tage billeder af andre passagerer i baggrunden eller omkring dem, samt ved at indsætte dedikerede køer, der er tydeligt mærket til ansigtsgenkendelse).

A.2.5 Hvis de samme standere kan anvendes af passagerer, der giver deres samtykke til ansigtsgenkendelse, og passagerer, der ikke giver deres samtykke, eller hvis passagerer, der ikke giver deres samtykke til ansigtsgenkendelse, kan ses i synsfeltet, mens systemet ikke anvendes, skal der afventes en positiv handling fra en passager, der giver sit samtykke, før optagelsen af foto eller video påbegyndes.

A.2.6 En registreret skal til enhver tid kunne foretage sletning af oplysninger, der kun er lagret hos vedkommende (biometrisk skabelon[65]), f.eks. i en mobilapplikation eller digital tegnebog[66].

A.2.7 Eksistensen af levedygtige alternativer eller backupløsninger (dvs. for passagerer, der ikke giver samtykke til brugen af deres biometriske data, for passagerer, der ikke kan bruge sådanne løsninger, eller for passagerer, der oplever falske afvisninger) for også at sikre, at passagerer, der ikke giver samtykke, ikke oplever nogen ulemper[67].

---

[63] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25, fodnote 60, punkt 70.
[64] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25, punkt 68, og betragtning 7 til GDPR.
[65] Henvisninger til den biometriske skabelon i garantierne i scenarie 1 svarer til henvisninger til nøglen/hemmeligheden i scenarie 2.
[66] Bemærk, at denne garanti kun gælder for scenarie 1.
[67] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 86.

A.2.8 Hvis der anvendes en applikation, bør den udformes og konfigureres omhyggeligt, så den ikke indsamler unødvendige data, og for at undgå brug af tredjepartssoftwareudviklingskit ("SDK"), der indsamler data til andre formål.

A.3 Ansvarlighed

A.3.1 Vurder, om der findes relevante adfærdskodekser eller certificeringsmekanismer, der kan bidrage til at påvise overholdelse af behandlingssikkerheden i artikel 32 i GDPR[68]. Verificer, om foranstaltningerne er hensigtsmæssige for den pågældende behandling. Standarder[69], bedste praksis og adfærdskodekser, som anerkendes af sammenslutninger og andre organer, der repræsenterer kategorier af dataansvarlige, kan være nyttige ved fastlæggelsen af passende foranstaltninger.

A.3.2 Sørg for, at der udføres grundlæggende sikkerhedskontroller på brugerens enhed for at muliggøre registreringsfasen, selv om passageren også medvirker ved beskyttelsen af sine data, da disse er lagret på enheden. Eksempler på sådanne tekniske kontroller findes nedenfor i afsnit C.2 "Infrastruktur og netværk".

B. Organisatoriske spørgsmål:

B.1 Politik og overensstemmelse

B.1.1. Sørg for, at interne adgangskontroller er på plads[70] med regler for administratorer.

B.1.2 Hvis ansigtsgenkendelsestjenesten kan leveres af en af de parter, der er involveret i behandlingen, uden at identifikationsdata eller biometriske data, eller begge typer data, skal håndteres af de andre involverede parter, forbydes det, at disse data strømmer gennem de andre parter. Et luftfartsselskab behøver f.eks. ikke teknisk at få adgang til de biometriske data, når det anvender lufthavnens fælles infrastruktur, selv om dette luftfartsselskab fungerer som dataansvarlig for behandlingen i henhold til GDPR.

B.1.3 Fastlæg en politik for kryptering og nøgleadministration[71], f.eks. til behandling af identifikationsdata og biometriske data.

B.1.4 Sørg for, at kapitel V i GDPR overholdes. Det sikres f.eks., at overførsler overholder reglerne, hvis den dataansvarlige under registreringsprocessen anvender en ekstern tjeneste, som er baseret i et tredjeland.

---

[68] Artikel 32, stk. 3, i GDPR og Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25, punkt 10.
[69] Se f.eks. ISO/IEC 2382-37.
[70] Databeskyttelsesrådets retningslinjer 04/2020 om brug af lokaliseringsdata og kontaktopsporingsredskaber i forbindelse med covid-19-udbruddet, vedtaget den 21.4.2020 ("**Databeskyttelsesrådets retningslinjer 04/2020 om lokaliseringsdata og kontaktopsporingsredskaber**"), SEC-10, s. 16.
[71] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 89.

B.1.5 Når der anvendes databehandlere, skal der indgås en databehandleraftale[72] i overensstemmelse med artikel 28, stk. 3, i GDPR.

B.1.6 Det sikres, at der er indført procedurer til styring af menneskeligt tilsyn og indgriben, især til håndtering af problemer med falsk afvisning, tekniske problemer eller problemer med anvendelsen.

B.2 Uddannelse og afprøvning

B.2.1. Det sikres, at personalet har den fornødne uddannelse.

B.2.2 Der gennemføres "en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed"[73].

B.2.3. Gennemfør en procedure for at sikre, at behandlingen af passagerens biometriske skabelon[74] til autentifikation er teknisk effektiv og tilstrækkelig nøjagtig.

B.2.4. Det sikres, at de biometriske prøver, der indsamles både ved registreringen og ved kontrolstedet, er af tilstrækkelig kvalitet til at foretage en pålidelig biometrisk behandling.

C. Tekniske spørgsmål:

C.1 Adgang

C.1.1 Garantier gennemføres i registreringsfasen for at sikre, at registreringen baseres på en verificeret identitet. For at styrke vurderingen af brugernes identitet kan der f.eks. gennemføres trin med multifaktorautentifikation, der spænder fra adgangskodebeskyttede engangslinks til aktivering af appen til mekanismer, der fjerner blokering på lokale enheder.

C.1.2 Gennemfør garantier for at håndtere tilfælde af falske positive resultater, præsentationsangreb og forebyggelse af svig[75].

C.1.3 Forbyd enhver ekstern adgang til identifikationsdata og biometriske data[76].

C.1.4 Sørg for, at behandlingen sker lokalt i faserne for registrering, transmission og matchning. Matchningspunktet bør være så tæt som muligt på personens enhed. For at skabelonen kan matches inden for den enkelte enhed, kan interaktion med tjenesteudbydere

[72] Artikel 28, stk. 3, i GDPR.
[73] Artikel 32, stk. 1, litra d), i GDPR.
[74] Henvisninger til den biometriske skabelon i garantierne i scenarie 1 svarer til henvisninger til nøglen/hemmeligheden i scenarie 2.
[75] ENISA Report on Digital Identity on leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust, januar 2022.
[76] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 89.

uden for lufthavnen og brug af offentlige netressourcer være nødvendig, og det kan påvirke tilgængeligheden og udbrede skabelonen til eksterne enheder.

C.1.5 En bruger autentificeres for at tilføje en ny flyvning og generere en ny krypteret QR-kode.

C.1.6 Gennemfør foranstaltninger til at håndtere situationen, hvor en passager mister adgangen til sin QR-kode.

C.2 Infrastruktur og netværk

C.2.1 Betingelserne for, at operativsystemet holdes ajour, og at autentifikation er aktiveret for adgang til enheden, så applikationen/den digitale tegnebog kan fungere, herunder automatisk sletning af identifikationsdata og biometriske data, hvis operativsystemet er forældet og udgør en sikkerhedsrisiko.

C.2.2 Isolering af enheder til matchning (dvs. standere) fra nettet under drift og iværksættelse af andre foranstaltninger, der er nødvendige for at garantere sikkerheden.

C.2.3 Udfør biometrisk matchning på passagerens enhed eller på standeren (edge computing).

C.2.4 Løsninger til at afhjælpe sikkerhedsmæssige sårbarheder i passagerernes individuelle enheder, herunder kryptering af (som minimum) biometriske data og identifikationsdata i dvaletilstand.

C.2.5 Anvend sikker lagring af (som minimum) biometriske data, der alene opbevares af brugeren[77], f.eks. ved at bruge Secure Enclave på en smartphone.

C.2.6 Sikkerhedsgarantier til sikring af lokalernes fysiske sikkerhed, herunder den biometriske terminal i lufthavnen. Det sikres, at der er et højt sikkerhedsniveau for de elementer i arkitekturen, der behandler identifikationsdata og biometriske data (f.eks. beregning, datastrøm, midlertidig lagring eller langvarig lagring).

C.3 Datasikkerhed og -styring i forbindelse med brugeridentitetskontrol

C.3.1 Opdel data under transmission og lagring i mindst tre forskellige grupper, f.eks.: identifikationsdata, biometriske data og flyoplysninger[78]. Sørg for, at dataene krypteres effektivt under både transmission og lagring.

C.3.2 Der indføres tekniske foranstaltninger for at sikre, at kun de data, der lovligt kan behandles ved specifikke kontrolsteder, behandles og kontrolleres ved kontrolstedet.

[77] Henvisninger til den biometriske skabelon i garantierne i scenarie 1 svarer til henvisninger til nøglen/hemmeligheden i scenarie 2.
[78] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 89.

C.3.3 Der sikres effektiv datasletning[79] gennem en sikker sletningsprocedure (f.eks. hovedhukommelse, cache og eventuelle sikkerhedskopier), og det vurderes, hvornår sletningen af data bør automatiseres. Datalagringsperioder bør håndhæves strengt ved hjælp af automatiske rutiner, uden at det er nødvendigt med en supplerende handling fra den enkeltes side[80].

C.3.4 Dataenes ægthed og integritet sikres (f.eks. underskrift)[81].

C.3.5 Passagerernes biometriske data opbevares kun på registreringsstedet og ved kontrolstedet i en meget kort periode, og de slettes, så snart passageren har passeret kontrolstedet.

C.3.6 Hvis en applikation bruges til registrering, anvendes sikkerhedsstandarder for mobilapplikationssikkerhed under udviklingen af applikationen samt sikkerhedstest udført af en tredjepart.

C.3.7 Det sikres, at der er indført sikkerhedsforanstaltninger i registreringsfasen i lufthavnen for at bevare fortroligheden og integriteten af passagerens biometriske data. Hvis QR-koden f.eks. udskrives af kiosken, bør QR-koden ikke vises i kiosken for at undgå, at en ondsindet aktør tager et billede. Ved transmission over korte afstande bør transmissionen udføres med brugerens aktive inddragelse og via en kanal, der sikrer nærhed.

C.3.8 Oplysninger, der alene opbevares af personen[82], bør opbevares sikkert på personens enhed, og eventuelle sårbarheder i forbindelse med enhedens operativsystemer skal underkastes relevante sikkerhedsopdateringer. Hvis QR-kode er udprintet, bør personen gøres opmærksom på den særligt følsomme karakter af de data, den indeholder, og hvad den gør det muligt at udføre.

C.3.9 Sørg for, at registreringen foretages ved hjælp af passende teknikker til fjernkontrol af identitet[83].

3.2.2 Scenarie 2: central lagring af registrerede biometriske skabeloner i krypteret form i lufthavnen og med en nøgle/hemmelighed alene hos passagererne med henblik på autentifikation

48. I dette afsnit undersøges det, om det er foreneligt med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR, at passagerers registrerede biometriske skabeloner lagres centralt i en central database

[79] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 89.
[80] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25, punkt 82.
[81] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 89.
[82] Henvisninger til den biometriske skabelon i garantierne i scenarie 1 svarer til henvisninger til nøglen/hemmeligheden i scenarie 2.
[83] Se ENISA Report on Remote ID Proofing: Analysis of methods to carry out identity proofing remotely, marts 2021.

i krypteret form og med en nøgle/hemmelighed, der udelukkende opbevares hos passageren[84] med henblik på autentifikation ("**scenarie 2**"). I dette afsnit undersøges også de fornødne garantier for scenarie 2 i lyset af artikel 25 og 32 i GDPR.

Beskrivelse af scenariet

49. I scenarie 2 foretages registrering kun én gang for en given gyldighedsperiode (f.eks. et år efter den sidste flyvning eller indtil passets udløbsdato), enten på afstand på et passende identitetssikringsniveau (f.eks. et passende eIDAS-sikringsniveau) eller i lufthavnsterminaler. Registreringen kontrolleres af lufthavnsoperatøren og består i at generere identifikationsdata og biometriske data, der krypteres med en nøgle/hemmelighed.

50. Databasen opbevares i lufthavnens lokaler under lufthavnsoperatørens kontrol. Individuelle krypteringsnøgler/hemmeligheder lagres kun på personens enhed (f.eks. i lufthavnsoperatørens mobilapp). Appen kan generere en QR-kode, der indeholder nøglen/hemmeligheden, som enten kan udskrives på papir eller vises på enhedens skærm[85]. Derudover udføres et andet lag af kryptering[86] af lufthavnsoperatøren med nøgler, der kontrolleres af lufthavnsoperatøren.

51. Passagererne verificeres (1:1-sammenligning), når de passerer specifikke kontrolsteder i lufthavnen. Passagerer, der vælger at gå gennem de biometriske kontrolsteder, fremviser deres QR-kode på en særlig kontrolstander, som er udstyret med en QR-scanner og et kamera. Passagerens indeks sendes til databasen for at anmode om den krypterede skabelon, som downloades og kontrolleres lokalt på kontrolstanderen og/eller brugerens enhed. Kun det matchende resultat kendes og anvendes af den dataansvarlige for kontrolstedet[87].

52. I dette scenarie er der ingen strømme af identifikationsdata og biometriske data mellem lufthavne, og der er hverken sammenkobling eller interoperabilitet mellem de centrale databaser.

Databeskyttelsesrådets vurdering

53. I scenarie 2 lagres passagerernes registrerede biometriske skabeloner centralt, men i krypteret form og med en nøgle/hemmelighed, der alene opbevares af passagererne. I scenarie 2 autentificeres passagererne (1:1 sammenligning).

54. I dette scenarie foreslås det, at målet om at strømline passagerstrømmen (dvs. ved hurtigere kontroller) kan nås ved hjælp af et centralt system. Databeskyttelsesrådet har tidligere bemærket, at en sådan løsning kan betragtes som et levedygtigt alternativ til decentral lagring af de registrerede biometriske skabeloner[88] (som beskrevet i scenarie 1), hvis der foreligger objektive behov, og der anvendes de fornødne garantier (se garantierne beskrevet i punkt 60 nedenfor).

---

[84] Som vist ved brugstilfælde 2 i bilag I til anmodningen.

[85] Den franske tilsynsmyndighed har yderligere præciseret, at der også kan være andre tekniske løsninger til at sende de krævede oplysninger, f.eks. ved at anvende en protokol til kortdistancekommunikation.

[86] Nøglen/hemmeligheden (hos personen) er selv krypteret med en anden nøgle, der opbevares af lufthavnsoperatøren.

[87] Den franske tilsynsmyndighed præciserede, at denne opbevaringsperiode er vejledende og kan anses for acceptabel, da nøglen opbevares af de enkelte personer og kan vælges i registreringsfasen. Det skal dog bemærkes, at en sådan opbevaringsperiode kan justeres.

[88] Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr, punkt 88.

55. Med hensyn til sikkerhed krypteres hver persons data med en specifik nøgle, som kun opbevares af personen selv og er under dennes enekontrol. Det forhold, at de oplysninger, der kræves til matchningen (dvs. hemmeligheden/nøglen), skal gives af personen, fungerer desuden som en anden faktor[89] og styrker dermed sikkerheden i forbindelse med autentifikationen. Derudover udføres et andet lag af kryptering af lufthavnsoperatøren med nøgler, der kontrolleres af lufthavnsoperatøren. I scenarie 2 sendes personens indeks til den centrale database for at hente de biometriske data, der er knyttet til personen. Disse data sendes derefter (i krypteret form) til en computer ved kontrolstedet, hvor de dekrypteres for at udføre matchningen, og kun det matchende resultat kendes og anvendes af kontrolløren på kontrolstedet. Såfremt personens nøgle/hemmelighed opbevares i en computer på kontrolstedet, og såfremt kun én passagers indeks sendes til den centrale database for at hente den krypterede biometriske skabelon, kan sådanne sikkerhedsforanstaltninger anses for at være forenelige med artikel 5, stk. 1, litra f), og artikel 32 i GDPR.

56. Med hensyn til foreneligheden med artikel 25 i GDPR og navnlig for at opfylde kravet om dataminimering bør det sikres, at behandlingen opfylder nødvendighedsprincippet. I scenarie 2 kan de valgte foranstaltninger anses for at have opfyldt nødvendighedsprincippet i forhold til det omhandlede mål (dvs. strømlining af passagerstrømmen i lufthavne), hvis den dataansvarlige – afhængigt af omstændighederne – kan påvise, at der ikke findes mindre indgribende alternative løsninger, der kan nå det samme mål lige så effektivt. I scenarie 2 skal passagererne stadig fremvise deres enhed[90]. Den dataansvarlige kan imidlertid eksempelvis påvise, at scenarie 2 fremskynder verifikationsprocessen i forhold til den nuværende situation, som omfatter en menneskelig kontrol af, om navnet på boardingkortet stemmer overens med passagerens identitetsdokument[91], eller i forhold til scenarie 1. Dette kan navnlig ikke påvises, hvis der i øjeblikket ikke foretages kontrol for at verificere passagerernes identitet på grundlag af deres officielle identitetsdokument (se i denne henseende punkt 18 ovenfor).

57. Med hensyn til proportionalitetsprincippet kan den indgribende karakter af en sådan behandling opvejes af passagerernes aktive inddragelse, da de har enekontrollen over nøglen til deres krypterede data. De sikkerhedsrisici, der er forbundet med lagringen af passagerernes biometriske data i en central database og med nøglen alene hos passagererne, kan tilsyneladende afbødes ved hjælp af fornødne garantier (se de garantier, der er omhandlet i punkt 60 nedenfor). Forudsat at den dataansvarlige gennemfører de fornødne garantier, der kræves i forbindelse med den pågældende specifikke behandling, kan risiciene for personer afbødes, og den negative indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder kan anses for at stå i et rimeligt forhold til den forventede fordel. Det bør naturligvis i hvert enkelt tilfælde sikres, at kun de oplysninger, der er nødvendige til formålet, behandles, og at kun passagerer, der har givet deres samtykke, kontrolleres, således at der ikke er risiko for, at der indsamles biometriske data om andre passagerer, der ikke har givet deres samtykke.

58. I anmodningen anføres det som eksempel, at opbevaringsperioden for de krypterede data i databasen i scenarie 2 typisk kan være et år efter den sidste flyvning, som personen har foretaget, og indtil

[89] Dette mindsker f.eks. risikoen for identitetsspoofing. Se også garanti C.1.2.

[90] Den franske tilsynsmyndighed har yderligere præciseret, at der også kan være andre muligheder for at fremvise en skabelon, f.eks. printet på papir. Databeskyttelsesrådet anerkender endvidere, at det i fremtiden kan overvejes at anvende en alternativ teknologi, f.eks. baseret på et Near Field Communication-system.

[91] Det kan også hævdes, at den biometriske kontrol kan gives anledning til færre fejl end en menneskelig kontrol.

passets udløbsdato. Der er ikke fremlagt oplysninger i anmodningen til støtte for en så lang periode begrundet i objektive forhold, selv om det kan antages, at en sådan opbevaringsperiode påtænkes for at lette fremtidige flyvninger. For at opnå forenelighed med artikel 5, stk. 1, litra e), i GDPR i dette scenarie bør de dataansvarlige kunne begrunde, hvorfor den påtænkte opbevaringsperiode er nødvendig til formålet i specifikke tilfælde. Databeskyttelsesrådet anbefaler, at de dataansvarlige anvender den kortest mulige opbevaringsperiode, også under hensyntagen til passagerer, der kun flyver meget sjældent, og tilbyder de registrerede at fastsætte deres foretrukne opbevaringsperiode.

59. I betragtning af ovenstående konkluderer Databeskyttelsesrådet derfor som svar på spørgsmål 2.1.1, at en sådan behandling **i princippet kan anses for at være forenelig med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR med forbehold af de fornødne garantier**.

Fornødne garantier

60. I denne type scenarie mener Databeskyttelsesrådet som svar på spørgsmål 2.1.2, at der som minimum bør gennemføres følgende garantier **ud over de garantier, der er anført i scenarie 1**. Andre garantier end dem, der er beskrevet i denne udtalelse, kan anvendes til at nå de samme sikkerheds- og databeskyttelsesmål og kan være lovlige, så længe de sikrer overholdelse af den gældende retlige ramme.

61. Bemærk: *Dette er en overordnet og ikke-udtømmende oversigt over de mulige fornødne garantier, som kan gennemføres af en dataansvarlig i en løsning svarende til scenarie 2. Hvorvidt de er hensigtsmæssige i henhold til artikel 25 og 32 i GDPR, afhænger af en konkret vurdering fra sag til sag. Alle dataansvarlige skal sikre, at de foretager deres egen konsekvensanalyse vedrørende databeskyttelse. Deres specifikke løsninger kan kræve yderligere foranstaltninger, som ikke er medtaget i denne udtalelse.*

D. Generelle spørgsmål

D.1 Registreredes rettigheder og garantier, der kan gennemføres af dataansvarlige

D.1.1 Det sikres, at passagerne har kontrol over opbevaringsperioderne for alle deres data. Opbevaringsperioderne bør begrænses til, hvad der er nødvendigt i forhold til det specifikke formål. Der bør fastsættes en maksimal periode på grundlag af en grundig analyse af faktorer som f.eks. identifikationsdokumentets gyldighed. De registrerede bør kunne fastsætte deres foretrukne opbevaringsperiode, som kan være kortere end standardopbevaringsperioden.

D.1.2 En registreret skal til enhver tid kunne anmode om at få slettet oplysninger, der kun er lagret hos vedkommende (nøgle/hemmelighed), f.eks. i en mobilapplikation eller digital tegnebog[92].

[92] Bemærk, at denne garanti kun gælder for scenarie 2.

D.1.3 Det sikres, at placeringen af den centrale database tillader den kompetente tilsynsmyndighed at føre effektivt tilsyn.

E. Organisatoriske spørgsmål:

E.1 Politik og overensstemmelse

E.1.1 Tilliden til den centrale server skal begrænses. Det sikres, at forvaltningen af den centrale server varetages i overensstemmelse med klart definerede forvaltningsregler og omfatter alle nødvendige foranstaltninger til at garantere dens sikkerhed[93].

F. Tekniske spørgsmål:

F.1 Adgang

F.1.1 Der føres logfiler over, hvem der har adgang til personoplysninger, navnlig identifikationsdata og biometriske data, og hvornår de blev tilgået.

F.2 Infrastruktur og netværk

F.2.1 Den centrale database sikres passende beskyttelse, herunder mod tilgængelighedsangreb.

F.2.2 Sørg for, at der ikke er internetforbindelse til den centrale database, registreringsstanderne og matchningsenhederne. Drift og vedligeholdelse af disse systemer (f.eks. backup, patching, overvågning osv.) skal udføres lokalt i lufthavnens lokaler.

F.3 Datasikkerhed og -styring

F.3.1 Der implementeres avancerede kryptografiske teknikker for at sikre udvekslingerne mellem applikationen og den centrale server[94].

F.3.2 Den enkelte nøgle/hemmelighed opbevares på det niveau, hvor den vil blive brugt til dekryptering (dvs. på standeren), og indekset bruges til at gendanne den tilsvarende registrerede biometriske skabelon i den centrale database.

F.3.3 Sørg for, at kommunikationen er beskyttet mod aflytning eller overførsel til tredjepart under udvekslingen af nøgle/hemmelighed mellem brugerenhed og standeren.

---

[93] Databeskyttelsesrådets retningslinjer 04/2020 om lokaliseringsdata og kontaktopsporingsredskaber, PRIV-5, s. 17.

[94] Databeskyttelsesrådets retningslinjer 04/2020 om lokaliseringsdata og kontaktopsporingsredskaber, SEC-4, s. 16: "Anvendelige teknikker er f.eks.: symmetrisk og asymmetrisk kryptering, hash-funktioner, Private Membership Test, Private Set Intersection, Bloom-filtre, Private Information Retrieval, homomorf kryptering osv.".

F.3.4 Den biometriske skabelon indekseres, når den er lagret i den centrale database, for at muliggøre 1:1-autentifikation og sikre, at den er unik og relateret til den pågældende person. Det sikres, at indekset ikke afslører nogen af passagerens identifikationsdata og ikke er korreleret med krypteringsnøglen.

F.3.5 Enhver transmission mellem den centrale database og kontrolstederne autentificeres og krypteres og overføres til isolerede netværk.

F.3.6 Undgå tovejslinks mellem datasæt (identifikationsdata og biometriske data samt flyoplysninger), og behold kun relevante envejslinks i databasen, f.eks. kun envejslinkene fra indeks til ID, fra indeks til krypterede biometriske data og fra indeks til flyoplysninger.

F.3.7 Der etableres ordninger for driftskontinuitet, f.eks. ved at have passende backuplagersystemer på plads.

F.3.8 Det sikres, at standeren ikke gemmer logfiler over de krypterede eller ukrypterede skabeloner.

3.2.3 Central lagring af de registrerede biometriske skabeloner med henblik på identifikation

62. I dette afsnit undersøges det, om det er foreneligt med artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR, at passagerers registrerede biometriske skabeloner lagres centralt, når sådanne skabeloner ikke er krypteret med en nøgle/hemmelighed, der udelukkende opbevares hos passageren med henblik på identifikation, i to brugstilfælde: 1) når sådanne skabeloner er lagret i en database i lufthavnen under lufthavnsoperatørens kontrol[95] ("**scenarie 3.1**"), og 2) når sådanne skabeloner er lagret i skyen under luftfartsselskabets kontrol[96] ("**scenarie 3.2**").

63. Databeskyttelsesrådet mener, at anvendelsen af biometriske data til **identifikation** i store centrale databaser griber ind i de registreredes grundlæggende rettigheder og kan få alvorlige konsekvenser for de registrerede[97]. Anvendelsen af biometriske data bør endvidere også undersøges i forhold til det formål, hvortil de behandles, i lyset af nødvendigheds- og proportionalitetsprincippet[98].

3.2.3.1 Scenarie 3.1: central lagring i en database i lufthavnen under lufthavnsoperatørens kontrol

Beskrivelse af scenariet

64. I scenarie 3.1 lagres passagerernes registrerede biometriske skabeloner i en central database i lufthavnens lokaler og under lufthavnsoperatørens kontrol i krypteret form. Passageroplysningerne er opdelt, dvs. at passagernes identifikationsdata, registrerede biometriske skabeloner og flyoplysninger

[95] Som vist ved brugstilfælde 3A i bilag I til anmodningen.
[96] Som vist ved brugstilfælde 3B bilag I til anmodningen.
[97] Se f.eks. Artikel 29-Gruppens udtalelse 3/2012 om biometriske teknologier, s. 8. Se også punkt 26 ovenfor.
[98] Betragtning 4 til GDPR. Se også Artikel 29-Gruppens udtalelse 3/2012 om biometriske teknologier, s. 8.

er lagret i tre forskellige databaser. Sådanne data krypteres med forskellige nøgler, både under lagringen og under overførslen til de servere, der udfører matchningen, hvor de derefter dekrypteres af lufthavnsoperatøren.

65. Passagererne skal registrere sig i forbindelse med hver flyvning kort tid før afgang (f.eks. 48 timer). En sådan registrering kan foretages enten på afstand eller i lufthavnsterminaler på et passende identitetssikringsniveau (f.eks. eIDAS på et passende sikringsniveau). Alternativt kan registreringen foretages som beskrevet i scenarie 1, hvor passagererne skal overføre deres data fra deres digitale tegnebøger til lufthavnssystemet inden for 48 timer før deres afgang.

66. Også i dette scenarie præsenterer passagererne sig foran en særlig kontrolstander, der er udstyret med et kamera. Deres biometriske prøve sendes derefter til en central server i lufthavnen, som forsøger at matche oplysningerne med den centrale biometriske database. Passageren kan således identificeres og kontrolleres for, om vedkommende rent faktisk er registreret til en flyafgang (eller til boarding i tilfælde af kontrol ved boarding). Afhængigt af kontrolstedet kan de oplysninger, der sendes tilbage til kontrolløren på kontrolstedet, minimeres, f.eks. som et "ja/nej svar" eller selve matchningsresultatet, hvis det er nødvendigt. I dette tilfælde sendes kun forespørgselsresultatet til og bruges af kontrolløren på kontrolstedet.

67. I dette scenarie identificeres navnlig passagererne (1:N-sammenligning), hvor N er det forventede antal passagerer i lufthavnen inden for en tidsramme på flere dage. Desuden foretages den biometriske matchning kun, når hver passager præsenterer sig på foruddefinerede kontrolsteder i afgangslufthavnen, men selve databehandlingen udføres på en central server, der er forbundet med den centrale database. Opbevaringsperioden i dette scenarie er typisk 48 timer, og dataene slettes, når flyet er lettet.

Databeskyttelsesrådets vurdering

68. Som nævnt ovenfor indebærer behandlingen af biometriske data øgede risici for de registreredes rettigheder og frihedsrettigheder[99]. Ethvert brud på datasikkerheden kan således have særligt alvorlige konsekvenser for de registrerede[100]. De dataansvarlige skal effektivt begrænse disse risici. Da hele arkitekturen i dette scenarie er fuldstændigt central, mister passagererne i højere grad kontrollen over deres data. Risikoen for, at oplysningerne ender med at blive behandlet til andre formål end kontrol af passagerstrømmen, kan desuden også være større.

69. I lyset af princippet om og kravene til sikkerhed (artikel 5, stk. 1, litra f), og artikel 32 i GDPR) bør det tages i betragtning, at lagring af identifikationsdata og biometriske data i centrale, men særskilte databaser kan udgøre betydelige angrebspunkter, og at brud på fortroligheden af en sådan database efterfølgende kan medføre adgang til hele datasættet. Som følge heraf kan et eventuelt sikkerhedsbrud i forbindelse med ansigtsgenkendelsesskabeloner og tilhørende identifikationsdata muliggøre uautoriseret eller ulovlig identifikation af de registrerede i andre miljøer. Det kan også, afhængigt af de metoder, der anvendes til biometrisk identifikation, true den fortsatte sikre anvendelse af ansigtsgenkendelsesskabeloner som identifikator. I så fald kan virkningerne af bruddet

[99] Se punkt 26 ovenfor.
[100] Guidelines on facial recognition, Europarådets rådgivende udvalg om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, juni 2021, s. 22.

ikke afbødes, i modsætning til en anden type legitimationsoplysninger (f.eks. bruger-ID eller adgangskode), som kan ændres[101].

70. Den store mængde og den høje kvalitet af identifikationsdata og biometriske data, som den dataansvarlige opbevarer, gør desuden denne til et meget værdifuldt mål for en angriber, hvilket med hensyn til sikkerhedsrisiko indebærer en højere grad af sandsynlighed. Brud på datasikkerheden kan desuden have større indvirkning, da det – fordi data lagres et centralt sted – kan være lettere for angribere at få adgang til personoplysninger vedrørende flere passagerer. Et muligt brud kan derfor potentielt udsætte et stort antal registrerede for store risici med hensyn til alvor, f.eks. identitetstyveri i stor skala, som er ekstremt vanskelige at afbøde.

71. Med hensyn til foreneligheden med artikel 5, stk. 1, litra f), og artikel 32 i GDPR er foranstaltningerne i scenarie 3.1[102] utilstrækkelige til at sikre et sikkerhedsniveau, der er passende i forhold til risikoen, med den nuværende teknologi. På dette grundlag vil behandlingen i henhold til scenarie 3.1 ikke være i overensstemmelse med artikel 5, stk. 1, litra f), og artikel 32 i GDPR, hvis en dataansvarlig begrænser sig til disse foranstaltninger.

72. I lyset af princippet i artikel 5, stk. 1, litra e), i GDPR er lagringsperioden for biometriske data i den centrale database i dette scenarie typisk 48 timer. En sådan begrænset opbevaringsperiode reducerer umiddelbart de risici, der er forbundet med brud på persondatasikkerheden, i væsentlig grad. Dataopbevaringsperioden er imidlertid ikke i sig selv en afgørende faktor for den nævnte arkitekturs overordnede forenelighed, da sådanne opbevaringsperioder kan ændres af de dataansvarlige. Under alle omstændigheder skal de foreslåede foranstaltninger opfylde kravene om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25 i GDPR.

73. I modsætning til scenarie 1 og 2, hvor passagererne autentificeres, identificeres passagererne i scenarie 3.1 (1:N-sammenligning), hvor N er det antal passagerer, der forventes i lufthavnen inden for en tidsramme på flere dage, og som har givet samtykke til en sådan behandling, når de passerer specifikke kontrolsteder i lufthavnen. Dette indebærer, at der søges efter passagerer i en central database, hvor hver indsamlet biometrisk prøve behandles for at kontrollere, om den matcher en person, der er kendt i systemet. I modsætning til scenarie 2 opbevares nøglerne i scenarie 3.1 ikke af passagererne alene. Derfor har passagererne i dette scenarie betydeligt mindre kontrol over deres biometriske data. En sådan behandling som foreslået i scenarie 3.1 kan derfor ikke anses for at være forenelig med kravene om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25 i GDPR.

74. I lyset af artikel 25 i GDPR bør dataansvarlige tage hensyn til de typer af, kategorier af og detaljeringsgrader for personoplysninger, der kræves til behandlingsformål[103]. Deres designvalg bør tage hensyn til de øgede risici for principperne om integritet, fortrolighed, dataminimering og opbevaringsbegrænsning ved indsamling af store mængder detaljerede personoplysninger og sammenligne dem med den risikoreduktion, der opnås ved at indsamle færre eller mindre detaljerede oplysninger om registrerede. Under alle omstændigheder må standardindstillingen ikke omfatte indsamling af personoplysninger, som ikke er nødvendige til det konkrete behandlingsformål. Med

[101] Se i denne forbindelse Artikel 29-Gruppens udtalelse 3/2012 om biometriske teknologier, s. 34.

[102] Som beskrevet i punkt 64-67 ovenfor.

[103] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger, punkt 49.

andre ord må der ikke indsamles overskydende personoplysninger, hvis visse kategorier af personoplysninger er unødvendige, eller hvis der ikke behøves detaljerede oplysninger, fordi det er tilstrækkeligt med mindre granulære data. Hvis en anden behandling kan anvendes til at nå det samme mål og er tilgængelig i henhold til de vilkår, der er beskrevet i scenarie 3.1, er det ikke nødvendigt at anvende ansigtsgenkendelse i dette tilfælde.

75. Med hensyn til artikel 25 i GDPR er et centralt element i databeskyttelse gennem design og standardindstillinger den registreredes autonomi. De registrerede bør have størst mulig autonomi til at afgøre, hvordan deres personoplysninger skal anvendes, i hvilket omfang og på hvilke vilkår[104]. I scenarie 1 ville de registrerede have autonomi og kontrol med hensyn til brugen, videregivelsen og sletningen af deres biometriske skabeloner, og i scenarie 2 ville de registrerede bevare en vis kontrol med hensyn til videregivelsen af deres egen biometriske skabelon, da de selv ville opbevare krypteringsnøglen/hemmeligheden. I scenarie 3.1 er de registrerede imidlertid fuldt ud afhængige af den dataansvarliges valg med hensyn til behandlingen af deres biometriske data og har derfor ingen direkte kontrol med hensyn til anvendelsen af deres biometriske skabelon.

76. Med hensyn til foreneligheden med artikel 25 i GDPR og navnlig for at opfylde kravet om dataminimering kan behandlingen i scenarie 3.1 ikke anses for at opfylde nødvendighedsprincippet. Databeskyttelsesrådet mener, at et lignende resultat med hensyn til at strømline passagerstrømmen i lufthavne kan opnås på en mindre indgribende måde. Dette kan f.eks. opnås uden brug af biometriske data (selv om brugeroplevelsen i så fald vil være anderledes, da det kan tage længere tid at fremvise boardingkort og om nødvendigt officielle identifikationsdokumenter). Andre løsninger, navnlig løsninger, der er baseret på lagring af biometriske data i en lokal tegnebog på personens enhed, eller løsninger, der kræver kryptering af dataene med en specifik nøgle, der er lagret på personens enhed, gør det endvidere muligt at nå målene på en mindre indgribende måde med hensyn til privatlivets fred.

77. Med hensyn til proportionalitetsprincippet vil den behandling, der er omhandlet i scenarie 3.1, skabe risici for de registreredes rettigheder, som ikke vil blive afbødet af de påtænkte foranstaltninger med den nuværende teknologi. Risikoen for en negativ indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder som følge af et brud på datasikkerheden i en central database med biometriske data for et stort antal personer synes at opveje den forventede fordel ved behandlingen, da en sådan fordel er relativt lille, dvs. en mindre forbedring med hensyn til bekvemmelighed og kontrolhastighed. Den kan derfor ikke begrunde disse foranstaltningers store indgriben i fysiske personers grundlæggende rettigheder og frihedsrettigheder, og den behandling, der er omhandlet i scenarie 3.1, opfylder ikke proportionalitetsprincippet.

78. Når behandlingen foretages med det specifikke formål at strømline passagerstrømmen i lufthavne, konkluderer Databeskyttelsesrådet som svar på spørgsmål 2.2.1 og i lyset af disse overvejelser, at den behandling, der er omhandlet i scenarie 3.1:

- **ikke kan anses for at være forenelig med artikel 25 i GDPR**

[104] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og standardindstillinger, punkt 70. I betragtning 7 til GDPR præciseres det yderligere, at "[f]ysiske personer bør have kontrol over deres personoplysninger".

- **ikke kan anses for at være i overensstemmelse med artikel 5, stk. 1, litra f), og artikel 32 i GDPR,** hvis en dataansvarlig begrænser sig til de foranstaltninger, der er beskrevet i scenarie 3.1.

3.2.3.2 Scenarie 3.2: central lagring i skyen under luftfartsselskabets kontrol

Beskrivelse af scenariet

79. I scenarie 3.2 lagres passagerernes registrerede biometriske skabeloner i skyen under luftfartsselskabets eller dets cloudtjenesteudbyders (databehandlers) kontrol. I anmodningen præciseres det, at cloudtjenesteudbyderen er beliggende i EØS[105]. I dette tilfælde krypteres passagerernes data, men dekrypteres, når de er i brug (f.eks. når matchningen udføres), og nøglerne kontrolleres af luftfartsselskabet eller dets cloudtjenesteudbyder. Passagerernes biometriske data anvendes til identifikation af passagererne (1:N-sammenligning), hvor N potentielt repræsenterer luftfartsselskabets samlede antal kunder[106].

80. I lighed med scenarie 1, 2 og 3.1 skal passagererne også her først registrere sig. I scenarie 3.2 foretages passagerernes registrering imidlertid kun én gang i den periode, hvor kunden har en konto hos luftfartsselskabet. Registreringen sker enten på afstand med et passende identitetssikringsniveau (f.eks. eIDAS med et passende sikringsniveau) eller i lufthavnsterminaler. Den biometriske matchning foretages kun, når hver passager præsenterer sig på foruddefinerede kontrolsteder i lufthavnen, men selve databehandlingen foretages i skyen.

81. I lufthavnen passerer passagererne særlige kontrolstandere, der er udstyret med et kamera. Passagerernes biometriske data sendes via en anmodning til et luftfartsselskabs cloudserver, hvor disse data matches i forhold til den centrale database. Passageren kan således identificeres og kontrolleres for, om vedkommende rent faktisk er registreret til en flyafgang (eller til boarding i tilfælde af kontrol ved boarding).

82. Matchningsresultaterne kan eventuelt stilles til rådighed for flere lufthavnsoperatører, hvis et luftfartsselskab har en særlig terminal eller adgang til en lufthavns fælles informationssysteminfrastruktur. Afhængigt af kontrolstedet kan de oplysninger, der sendes tilbage til kontrolløren på kontrolstedet, minimeres, f.eks. som et "ja/nej svar" eller selve matchningsresultatet, hvis det er nødvendigt. I dette tilfælde der det kun kontrolløren på kontrolstedet, der kender forespørgselsresultatet og anvender det.

83. Opbevaringsperioden for skabelonen fastsættes af luftfartsselskabet og kan potentielt vare, så længe kunden har en konto hos selskabet.

Databeskyttelsesrådets vurdering

84. De overvejelser, som Databeskyttelsesrådet allerede har givet udtryk for i forbindelse med scenarie 3.1[107], gælder også for dette scenarie.

85. Med hensyn til princippet om og kravene til sikkerhed (artikel 5, stk. 1, litra f), og artikel 32 i GDPR) foretages behandlingen i scenarie 3.2 i skyen, og flere enheder kan have adgang til sådanne data,

[105] Den franske tilsynsmyndighed præciserede, at dette er vejledende, og at cloudtjenesteudbydere, der ikke er beliggende i EØS, også kan overvejes. Andre lagringsløsninger (f.eks. uden brug af cloud) kan også overvejes.
[106] Den franske tilsynsmyndighed præciserede, at dette er vejledende, og at der findes en løsning, hvor biometriske data sendes hver gang forud for flyafgangen.
[107] Punkt 68-77 ovenfor.

herunder også udbydere uden for EØS, selv når dataene opbevares i EØS[108]. En sådan arkitektur indebærer potentielle risici ved overførsel af personoplysninger til tredjelande. Selv om passagerernes data er krypterede, dekrypteres de, når de er i brug (f.eks. når matchningen udføres), og nøglerne kontrolleres af luftfartsselskabet eller dets cloudtjenesteudbyder. En sådan opbevaring kan føre til en yderligere forøgelse af sikkerhedsrisikoen.

86. Med hensyn til foreneligheden med artikel 5, stk. 1, litra f), og artikel 32 i GDPR er foranstaltningerne i scenarie 3.2[109] utilstrækkelige til at sikre et sikkerhedsniveau, der er passende i forhold til risikoen, med den nuværende teknologi. På dette grundlag vil behandlingen i henhold til scenarie 3.2 ikke være i overensstemmelse med artikel 5, stk. 1, litra f), og artikel 32 i GDPR, hvis en dataansvarlig begrænser sig til disse foranstaltninger.

87. Det fremgår endvidere af scenarie 3.2[110], at oplysningerne kan opbevares i en betydelig periode (dvs. potentielt så længe den registrerede har en konto hos luftfartsselskabet). En sådan opbevaringsperiode udsætter dataene for en større risiko for sikkerhedsbrud, som tilsyneladende går ud over, hvad der er strengt nødvendigt og forholdsmæssigt med henblik på behandlingen. Databeskyttelsesrådet bemærker, at dataopbevaringsperioden ikke i sig selv er en afgørende faktor for den nævnte arkitekturs overordnede forenelighed med GDPR, da den kan ændres af de dataansvarlige. På grundlag af de oplysninger, som Databeskyttelsesrådet har til rådighed, og som er indeholdt i beskrivelsen af scenarie 3.2, er der imidlertid ikke en tilstrækkelig begrundelse for denne lange opbevaringsperiode, og der er ingen åbenbare foranstaltninger til at mindske risiciene for registrerede. På dette grundlag er den foreslåede opbevaringsperiode ikke begrænset til, hvad der er nødvendigt, i henhold til princippet om opbevaringsbegrænsning i artikel 5, stk. 1, litra e), i GDPR.

88. Under alle omstændigheder kan de foreslåede foranstaltninger i scenarie 3.2 ikke anses for at opfylde kravene om databeskyttelse gennem design og standardindstillinger i henhold til artikel 25 i GDPR. I scenarie 3.2 lagres passagerernes registrerede biometriske skabeloner i skyen under luftfartsselskabets eller dets cloudtjenesteudbyders (databehandlers) kontrol. Som beskrevet ovenfor kan flere enheder potentielt have adgang til disse data. Passagerernes biometriske data anvendes desuden til identifikation af passagererne (1:N-sammenligning), hvor N potentielt repræsenterer luftfartsselskabets samlede antal brugere/kunder. Denne metode indebærer, at findes en person blandt en gruppe af personer i den centrale database, ved at behandle hvert opfanget ansigt for at kontrollere, om det matcher med en person, der er kendt af systemet. I modsætning til scenarie 3.1 kan sammenligningen i scenarie 3.2 foretages i meget større målestok, da kriteriet her er luftfartsselskabets samlede antal kunder, mens scenarie 3.1 kun omfattede det forventede antal passagerer inden for en tidsramme på flere dage.

89. Med hensyn til foreneligheden med artikel 25 i GDPR og navnlig for at opfylde kravet om dataminimering kan behandlingen i scenarie 3.2 ikke anses for at opfylde nødvendighedsprincippet. Databeskyttelsesrådet mener, at et lignende resultat med hensyn til at strømline passagerstrømmen i lufthavne kan opnås ved hjælp af andre mindre indgribende foranstaltninger, f.eks. uden brug af biometriske data, selv om brugeroplevelsen så ville være anderledes, da det kan tage længere tid at

[108] Databeskyttelsesrådets koordinerede håndhævelsestiltag 2022 vedrørende den offentlige sektors brug af cloudbaserede tjenester, 17.1.2023, s. 19.
[109] Se punkt 79-83 ovenfor.
[110] Se punkt 83 ovenfor.

fremvise ID-kort og boardingkort. Andre løsninger, navnlig løsninger, der er baseret på lagring af biometriske data i en lokal tegnebog på personens enhed, eller løsninger, der kræver kryptering af dataene med en specifik nøgle, der er lagret på personens enhed, gør det endvidere muligt for den dataansvarlige at nå målene på en mindre indgribende måde med hensyn til privatlivets fred.

90. Med hensyn til proportionalitetsprincippet vil den behandling, der er omhandlet i scenarie 3.2, skabe risici for de registreredes rettigheder, som ikke vil blive afbødet af de påtænkte garantier. Den negative indvirkning på de registreredes grundlæggende rettigheder og frihedsrettigheder som følge af et brud på datasikkerheden i en central database med biometriske data for et stort antal personer, som er lagret i skyen, synes at opveje den forventede fordel ved behandlingen, da en sådan fordel er relativt lille, dvs. en mindre forbedring med hensyn til bekvemmelighed og kontrolhastighed. Den kan derfor ikke begrunde disse foranstaltningers store indgriben i fysiske personers grundlæggende rettigheder og frihedsrettigheder, og den behandling, der er omhandlet i scenarie 3.2, kan ikke anses for at opfylde proportionalitetsprincippet.

91. Når behandlingen foretages med det specifikke formål at strømline passagerstrømmen i lufthavne, konkluderer Databeskyttelsesrådet som svar på spørgsmål 2.3.1 og i lyset af disse overvejelser, at den behandling, der er omhandlet i scenarie 3.2:

- **ikke kan anses for at være forenelig med artikel 25 i GDPR**
- **ikke kan anses for at være i overensstemmelse med artikel 5, stk. 1, litra f), og artikel 32 i GDPR**, hvis en dataansvarlig begrænser sig til de foranstaltninger, der er beskrevet i scenarie 3.2
- **ikke kan anses for at være i overensstemmelse med artikel 5, stk. 1, litra e), i GDPR**, da der ikke er en tilstrækkelig begrundelse for den opbevaringsperiode, der er fastsat i scenarie 3.2, baseret på de oplysninger, som Databeskyttelsesrådet har til rådighed. For at overholde princippet om opbevaringsbegrænsning i artikel 5, stk. 1, litra e), i GDPR skal den dataansvarlige påvise, at personoplysninger ikke lagres længere end nødvendigt til de formål, hvortil de behandles.

4 KONKLUSIONER

92. Med hensyn til spørgsmål 1.1 konkluderer Databeskyttelsesrådet på grundlag af anmodningen om en udtalelse fra den franske tilsynsmyndighed i forbindelse med kravene i artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR og på grundlag af ovenstående analyse, at:

93. brugen af ansigtsgenkendelsesteknologi til biometrisk autentifikation med det specifikke formål at strømline passagerstrømmen i lufthavne (sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge) kan anses for at være forenelig med principperne om integritet og fortrolighed i artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR i tilfælde af en lagringsarkitektur, hvor den registrerede biometriske skabelon for hver passager er lagret lokalt på vedkommendes individuelle enhed og under dennes enekontrol, hvis de fornødne garantier som beskrevet i punkt 46 ovenfor er gennemført.

94. Med hensyn til spørgsmål 2.1.1 konkluderer Databeskyttelsesrådet på grundlag af anmodningen om en udtalelse fra den franske tilsynsmyndighed i forbindelse med kravene i artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR og på grundlag af ovenstående analyse, at:

95. brugen af ansigtsgenkendelsesteknologi til biometrisk autentifikation med det specifikke formål at strømline passagerstrømmen i lufthavne (sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge) kan anses for at være forenelig med princippet om opbevaringsbegrænsning i artikel 5, stk. 1, litra e), i GDPR og principperne om integritet og fortrolighed i artikel 5, stk. 1, litra f), samt artikel 25 og 32 i GDPR i tilfælde af en central lagringsarkitektur, hvor hver passagers registrerede biometriske skabelon er lagret i en central database i lufthavnen under lufthavnsoperatørens kontrol i krypteret form med en nøgle/hemmelighed, der udelukkende opbevares af personen selv, hvis de fornødne garantier som beskrevet i punkt 60 ovenfor er gennemført.

96. Med hensyn til spørgsmål 2.2.1 konkluderer Databeskyttelsesrådet på grundlag af anmodningen om en udtalelse fra den franske tilsynsmyndighed vedrørende kravene i artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR og på grundlag af ovenstående analyse, at:

97. brugen af ansigtsgenkendelsesteknologi til biometrisk identifikation med det specifikke formål at strømline passagerstrømmen i lufthavne (sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge) i tilfælde af en central lagringsarkitektur, hvor passagerers registrerede biometriske skabeloner ikke er krypteret med en nøgle/hemmelighed, der udelukkende opbevares hos passageren, hvis sådanne skabeloner er lagret i en database i lufthavnen (under lufthavnsoperatørens kontrol), ikke kan anses for at være forenelig med artikel 25 i GDPR. En sådan behandling kan heller ikke anses for at være i overensstemmelse med principperne om integritet og fortrolighed i artikel 5, stk. 1, litra f), og artikel 32 i GDPR, hvis en dataansvarlig begrænser sig til de foranstaltninger, der er beskrevet i scenarie 3.1.

98. Med hensyn til spørgsmål 2.3.1 konkluderer Databeskyttelsesrådet på grundlag af anmodningen om en udtalelse fra den franske tilsynsmyndighed vedrørende kravene i artikel 5, stk. 1, litra e) og f), samt artikel 25 og 32 i GDPR og på grundlag af ovenstående analyse, at:

99. brugen af ansigtsgenkendelsesteknologi til biometrisk identifikation med det specifikke formål at strømline passagerstrømmen i lufthavne (sikkerhedskontrol, bagageindlevering, boarding og adgang til passagerlounge) i tilfælde af en central lagringsarkitektur, hvor passagerers registrerede biometriske skabeloner ikke er krypteret med en nøgle/hemmelighed, der udelukkende opbevares hos passageren, hvis sådanne skabeloner er lagret i skyen (under luftfartsselskabets kontrol), ikke kan anses for at være forenelig med artikel 25 i GDPR. En sådan behandling kan heller ikke anses for at være i overensstemmelse med principperne om integritet og fortrolighed i artikel 5, stk. 1, litra f), og artikel 32 i GDPR, hvis en dataansvarlig begrænser sig til de foranstaltninger, der er beskrevet i scenarie 3.2. Endelig kan behandlingen på grundlag af beskrivelsen af scenarie 3.2 og de oplysninger, som Databeskyttelsesrådet har til rådighed, ikke anses for være i overensstemmelse med princippet om opbevaringsbegrænsning i artikel 5, stk. 1, litra e), i GDPR.

På Det Europæiske Databeskyttelsesråds vegne

Formand

(Anu Talus)