Advies van de EDPB (artikel 64)

Advies 11/2024 betreffende het gebruik van gezichtsherkenning om de passagiersstroom op luchthavens te stroomlijnen (verenigbaarheid met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG)

Versie 1.1

Vastgesteld op 23 mei 2024

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

Vastgesteld

Versie 1.1	28 mei 2024	Grammaticale correctie in de samenvatting (bladzijden 3 en 4) en de punten 77 en 90 van het advies
Versie 1.0	23 mei 2024	Vaststelling van het advies

Samenvatting

De Franse toezichthoudende autoriteit heeft het Europees Comité voor gegevensbescherming verzocht een advies uit te brengen over het gebruik van gezichtsherkenningstechnologie door luchthavenexploitanten en luchtvaartmaatschappijen voor de biometrische authenticatie of identificatie van passagiers om de passagiersstroom op luchthavens te stroomlijnen.

Om te beginnen herinnert het Comité eraan dat het gebruik van biometrische gegevens, en met name gezichtsherkenningstechnologie, verhoogde risico's voor de rechten en vrijheden van betrokkenen met zich meebrengt. Het betreft de verwerking van biometrische gegevens, die bijzondere bescherming genieten op grond van artikel 9 AVG. Alvorens gebruik te maken van dergelijke technologieën, zelfs indien deze als bijzonder doeltreffend zouden worden beschouwd, moeten verwerkingsverantwoordelijken de gevolgen voor de grondrechten en de fundamentele vrijheden van betrokkenen beoordelen en moeten zij nagaan of het legitieme doel van de verwerking met minder indringende middelen kan worden bereikt.

Het toepassingsgebied van dit advies is, overeenkomstig het verzoek, beperkt tot de verenigbaarheid van de verwerking met **artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG** met het **specifieke doel om de passagiersstroom op luchthavens te stroomlijnen** bij vier specifieke controleposten, namelijk bij de beveiligingscontroleposten, het inchecken van bagage, het instappen en de toegang tot de passagierslounge. Dit advies bevat geen volledige en complete analyse van de naleving van de AVG door de desbetreffende verwerkingsverantwoordelijke(n) of zijn/hun eventuele verwerker(s) in elk mogelijk geval. Het advies laat een juridische en technische analyse per geval op basis van de door een verwerkingsverantwoordelijke beoogde specifieke verwerking en de omstandigheden dan ook onverlet. Bovendien valt de analyse van de toepasselijke rechtsgrondslag niet binnen de reikwijdte van de vragen die in het verzoek aan het Comité worden voorgelegd, en bijgevolg wordt de geldigheid van toestemming voor een dergelijke verwerking, overeenkomstig de artikelen 6, 7 en 9 AVG, in dit advies niet onderzocht. Voorts laat het onderhavige advies de in het lidstatelijke recht vastgelegde beperkingen op het gebruik van biometrische gegevens onverlet.

In dit advies beoordeelt het Comité of de verwerking in overeenstemming is met de bovenstaande bepalingen van de AVG in de context van **vier specifieke scenario's**.

Het **eerste scenario** betreft de opslag van een geregistreerde biometrische template in handen van het individu, bijvoorbeeld op zijn persoonlijke apparaat, onder zijn uitsluitende controle, om de passagier te authenticeren (één-op-éénvergelijking) wanneer deze door de bovengenoemde controleposten op de luchthaven gaat.

Het Comité concludeert dat de gekozen maatregelen kunnen worden geacht aan het noodzaakbeginsel te hebben voldaan indien de verwerkingsverantwoordelijke kan aantonen dat er geen minder indringende alternatieve oplossingen zijn waarmee op even doeltreffende wijze hetzelfde doel zou kunnen worden bereikt. Daarnaast kan de indringendheid van de verwerking worden gecompenseerd door de actieve betrokkenheid van de passagiers aangezien hun biometrische template alleen in hun handen wordt opgeslagen, bijvoorbeeld op hun persoonlijke apparaat, onder hun uitsluitende controle, en hun gegevens kort na de matching worden gewist. Op grond van het bovenstaande concludeert het Comité dat de in het eerste scenario beoogde verwerking **in beginsel verenigbaar kan worden geacht met artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG**, mits passende waarborgen worden geboden.

Het Comité heeft waarborgen geïdentificeerd waarin ten minste moet worden voorzien om tot een oplossing te komen die vergelijkbaar is met die in het eerste scenario.

Het **tweede scenario** betreft de gecentraliseerde opslag, binnen de luchthaven, van een geregistreerde biometrische template in versleutelde vorm met een sleutel/geheim die/dat uitsluitend in handen is van de passagier. Dit maakt de authenticatie van passagiers (één-op-éénvergelijking) mogelijk wanneer zij door de bovengenoemde controleposten op de luchthaven gaan. De registratie is geldig gedurende een bepaalde periode, bijvoorbeeld tot één jaar na de laatste vlucht tot aan de vervaldatum van het paspoort.

Het Comité concludeert dat de verwerking kan worden geacht aan het noodzaakbeginsel te hebben voldaan indien de verwerkingsverantwoordelijke kan aantonen dat er geen minder indringende alternatieve oplossingen zijn waarmee op even doeltreffende wijze hetzelfde doel kan worden bereikt. Bovendien kan de indringendheid van de verwerking worden gecompenseerd door de actieve betrokkenheid van de passagier aangezien deze de sleutel/het geheim tot zijn versleutelde biometrische gegevens onder zijn uitsluitende controle houdt. Ervan uitgaande dat de verwerkingsverantwoordelijke passende waarborgen invoert, kunnen de uit het gebruik van een gecentraliseerde databank voortvloeiende beveiligingsrisico's in dit scenario worden beperkt en kunnen de negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van de betrokkenen als evenredig aan het verwachte voordeel worden beschouwd. Wat het beginsel van opslagbeperking betreft, is er geen informatie aan het Comité verstrekt om de lange opslagperiode te onderbouwen. Met het oog op de verenigbaarheid met artikel 5, lid 1, punt e), AVG in dit scenario moeten de verwerkingsverantwoordelijken kunnen rechtvaardigen waarom de beoogde bewaartermijn in specifieke gevallen noodzakelijk is voor het doel van de verwerking. Het Comité beveelt aan dat verwerkingsverantwoordelijken de kortst mogelijke opslagperiode nastreven en tegelijkertijd passagiers de mogelijkheid bieden de opslagperiode van hun voorkeur in te stellen. Op grond van het bovenstaande concludeert het Comité dat de in het tweede scenario beoogde verwerking **in beginsel verenigbaar kan worden geacht met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG**, mits passende waarborgen worden geboden.

Het Comité heeft waarborgen geïdentificeerd waarin ten minste moet worden voorzien om tot een oplossing te komen die vergelijkbaar is met die in het tweede scenario.

Het **derde scenario** betreft de gecentraliseerde opslag van een geregistreerde biometrische template in versleutelde vorm binnen de luchthaven onder de controle van de luchthavenexploitant. Dit maakt de identificatie van passagiers (één-op-n-vergelijking) mogelijk wanneer zij door de bovengenoemde controleposten op de luchthaven gaan. De opslagperiode in dit scenario bedraagt doorgaans 48 uur en de gegevens worden gewist zodra het vliegtuig is vertrokken.

Aangezien de ID- en biometrische gegevens in een centrale databank worden opgeslagen, kan een schending van de vertrouwelijkheid van de databank ertoe leiden dat vervolgens toegang wordt verkregen tot de gehele dataset, waardoor ongeoorloofde of onrechtmatige identificatie van passagiers in andere omgevingen mogelijk wordt. De gecentraliseerde opslagarchitectuur onder de controle van de luchthavenexploitant leidt er bovendien toe dat de passagier in grotere mate de controle over zijn gegevens verliest. Het Comité is van mening dat een met het stroomlijnen van de passagiersstroom op luchthavens vergelijkbaar resultaat op een minder indringende manier kan worden bereikt en dat de negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van de betrokkenen die uit een inbreuk in verband met persoonsgegevens in een gecentraliseerde databank met biometrische gegevens zouden voortvloeien, zwaarder lijken te wegen dan het verwachte voordeel dat uit de verwerking voortvloeit. De verwerking kan derhalve niet voldoen aan

de noodzaak- en evenredigheidsbeginselen. Op grond van het bovenstaande concludeert het Comité dat de in het derde scenario beoogde verwerking **niet verenigbaar kan zijn met artikel 25 AVG**. Bovendien zou de verwerking **niet voldoen aan artikel 5, lid 1, punt f), en artikel 32 AVG** indien een verwerkingsverantwoordelijke zich tot de in dit scenario beschreven maatregelen zou beperken.

Het **vierde scenario** betreft de gecentraliseerde opslag van een geregistreerde biometrische template in versleutelde vorm in de cloud onder de controle van de luchtvaartmaatschappij of haar cloudaanbieder. Dit maakt de identificatie van passagiers (één-op-n-vergelijking) mogelijk wanneer zij door de bovengenoemde controleposten op de luchthaven gaan. De opslagperiode kan in dit scenario zo lang zijn als de klant een account aanhoudt bij de luchtvaartmaatschappij.

Aangezien de ID- en biometrische gegevens in een centrale databank in de cloud worden opgeslagen, kunnen meerdere entiteiten toegang hebben tot deze gegevens, waaronder mogelijk niet-EER-aanbieders. De gegevens van de passagier worden tijdens het gebruik gedecodeerd en de sleutels vallen onder de controle van de luchtvaartmaatschappij of haar verwerkers, wat de blootstelling aan beveiligingsrisico's zou kunnen verhogen. Een dergelijke gecentraliseerde opslagarchitectuur leidt er bovendien toe dat de passagier in grotere mate de controle over zijn gegevens verliest. De gegevens zouden ook gedurende een aanzienlijke periode kunnen worden opgeslagen, waardoor zij worden blootgesteld aan een hoger risico van een beveiligingsinbreuk en mogelijk langer worden bewaard dan strikt noodzakelijk en evenredig is met het oog op de verwerking, tenzij er verdere maatregelen worden genomen om de risico's voor individuen te beperken.

Het Comité is van mening dat een met het stroomlijnen van de passagiersstroom op luchthavens vergelijkbaar resultaat op een minder indringende manier kan worden bereikt en dat de negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van de betrokkenen die uit een inbreuk in verband met persoonsgegevens in een gecentraliseerde databank met biometrische gegevens kunnen voortvloeien, zwaarder lijken te wegen dan het verwachte voordeel dat uit de verwerking voortvloeit. De verwerking kan derhalve niet voldoen aan de noodzaak- en evenredigheidsbeginselen. Op grond van het bovenstaande concludeert het Comité dat de in het vierde scenario beoogde verwerking **niet verenigbaar kan zijn met artikel 25 AVG**. Bovendien zou de verwerking, op basis van de informatie die het Comité ter beschikking staat, **niet voldoen aan artikel 5, lid 1, punt e), AVG** en **evenmin aan artikel 5, lid 1, punt f), en artikel 32 AVG** indien een verwerkingsverantwoordelijke zich tot de in dit scenario beschreven maatregelen zou beperken.

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 63 en artikel 64, lid 2, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "**AVG**"),

Gezien de EER-Overeenkomst en met name bijlage XI en Protocol 37, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien de artikelen 10 en 22 van het reglement van orde (hierna het "**rvo EDPB**") van het Europees Comité voor gegevensbescherming (hierna het "**Comité**" of de "**EDPB**"),

Overwegende hetgeen volgt:

1) De belangrijkste rol van het Comité is te zorgen voor een consistente toepassing van de AVG in de gehele Europese Economische Ruimte (hierna "**EER**"). In artikel 64, lid 2, AVG is bepaald dat een toezichthoudende autoriteit (hierna "**TA**"), de voorzitter van het Comité of de Europese Commissie elk kunnen verzoeken dat aangelegenheden van algemene strekking of met rechtsgevolgen in meer dan één EER-lidstaat worden onderzocht door het Comité teneinde advies te verkrijgen.

2) Het advies van het Comité wordt overeenkomstig artikel 64, lid 3, AVG, in samenhang met artikel 10, lid 2, van het rvo EDPB, vastgesteld binnen acht weken nadat de voorzitter en de bevoegde TA hebben besloten dat het dossier volledig is. Die termijn kan door de voorzitter met zes weken worden verlengd, rekening houdend met de complexiteit van de aangelegenheid.

Brengt het volgende advies uit:

1 INLEIDING

1.1 Overzicht van de feiten

1. Op 16 februari 2024 heeft de Franse toezichthoudende autoriteit (hierna de "**FR TA**") het Comité verzocht een advies uit te brengen over de verenigbaarheid met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG van het gebruik van gezichtsherkenningstechnologie door luchthavenexploitanten en luchtvaartmaatschappijen voor de biometrische authenticatie of identificatie van passagiers[2], met het oog op het stroomlijnen van de passagiersstroom, bij de beveiligingscontroleposten op luchthavens[3], het inchecken van bagage, het instappen en de toegang tot de passagierslounge (met uitzondering van grenscontroles en door belastingvrije winkels

[1] Met "**lidstaten**" worden in dit advies "lidstaten van de EER" bedoeld. Met "de Unie" of "EU" wordt in dit advies "de EER" bedoeld.
[2] In de context van dit advies wordt met "**passagier**" een betrokkene bedoeld wiens persoonsgegevens worden verwerkt voor het in dit advies beschreven specifieke doel. De termen "passagier" en "individu" worden hierna in dit advies door elkaar gebruikt.
[3] Voor het onderhavige advies worden onder "**beveiligingscontroleposten op luchthavens**" de onder de verantwoordelijkheid van de luchthavenexploitant uitgevoerde beveiligingscontroles verstaan waaraan passagiers worden onderworpen als zij van de vertrekhal naar de instapzone of de boarding gate gaan.

uitgevoerde controles) (hierna het "**verzoek**"). De FR TA heeft bij haar verzoek een beschrijving van typische gebruiksgevallen gevoegd (bijlage I).

2. In haar verzoek merkt de FR TA op dat de modellen die momenteel op verschillende EU-luchthavens worden getest, van lidstaat tot lidstaat verschillen. Dit kan het risico van uiteenlopende interpretaties tussen de TA's met zich meebrengen, evenals het risico dat er verschillende gevolgen optreden voor de grondrechten en de fundamentele vrijheden van betrokkenen in de EU[4].

3. Het Comité is van mening dat, om op het verzoek te kunnen reageren, de volgende vragen moeten worden beantwoord:

4. **Vraag 1:**

1.1. Kan het gebruik van gezichtsherkenningstechnologie voor biometrische authenticatie **met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen** (beveiligingscontroleposten, het inchecken van bagage, het instappen en de toegang tot de passagierslounge) verenigbaar zijn met **artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG** in het geval van een opslagarchitectuur waarbij de biometrische template van elke passagier **alleen in handen van het individu** wordt opgeslagen, bijvoorbeeld lokaal op zijn persoonlijke apparaat, onder zijn uitsluitende controle?

1.2. Indien een dergelijke verwerking met de bovengenoemde bepalingen verenigbaar zou worden bevonden, welke minimale passende waarborgen zouden er dan nodig zijn in het licht van de artikelen 25 en 32 AVG?

Vraag 2:

2.1. Kan het gebruik van gezichtsherkenningstechnologie voor biometrische authenticatie of identificatie **met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen** (beveiligingscontroleposten, het inchecken van bagage, het instappen en de toegang tot de passagierslounge) verenigbaar zijn met **artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG** in het geval van een **gecentraliseerde** opslagarchitectuur waarbij de biometrische template van elke passagier wordt opgeslagen in een centrale databank:

2.1.1. In een centrale databank binnen de luchthaven, onder de controle van de luchthavenexploitant, in versleutelde vorm, met een sleutel/geheim die/dat uitsluitend in handen is van het individu (bijvoorbeeld op de mobiele telefoon van het individu), voor authenticatie?

2.1.2. Indien een dergelijke verwerking verenigbaar zou worden bevonden, welke minimale passende waarborgen zouden er dan nodig zijn in het licht van de artikelen 25 en 32 AVG?

2.2.1. In een centrale databank binnen de luchthaven, onder de controle van de luchthavenexploitant, in versleutelde vorm, met sleutels die in handen zijn van de luchthavenexploitant, voor identificatie?

[4] Verzoek, blz. 1.

2.2.2. Indien een dergelijke verwerking verenigbaar zou worden bevonden, welke minimale passende waarborgen zouden er dan nodig zijn in het licht van de artikelen 25 en 32 AVG?

2.3.1. In de cloud, onder de controle van de luchtvaartmaatschappij of haar dienstverlener (verwerker), in versleutelde vorm, met sleutels die in handen zijn van de luchtvaartmaatschappij of haar dienstverlener, voor identificatie?

2.3.2. Indien een dergelijke verwerking verenigbaar zou worden bevonden, welke minimale passende waarborgen zouden er dan nodig zijn in het licht van de artikelen 25 en 32 AVG?

5. Nadat de FR TA op 16 februari 2024 het dossier als volledig had beschouwd en de voorzitter van het Comité op 23 februari 2024 het dossier als volledig had beschouwd, werd het dossier op 23 februari 2024 door het secretariaat doorgezonden. Gelet op de complexiteit van de aangelegenheid, besloot de voorzitter van het Comité, in overeenstemming met artikel 64, lid 3, AVG, juncto artikel 10, lid 2, rvo EDPB, om de standaardtermijn van acht weken met zes weken te verlengen.

1.2 Ontvankelijkheid van het verzoek om een advies uit hoofde van artikel 64, lid 2, AVG

6. In artikel 64, lid 2, AVG is met name bepaald dat een TA, de voorzitter van het Comité of de Commissie elk kunnen verzoeken dat aangelegenheden van algemene strekking of met rechtsgevolgen in meer dan één lidstaat worden onderzocht door het Comité teneinde advies te verkrijgen.

7. Het Comité is van mening dat het verzoek van de FR TA betreffende de verenigbaarheid van het gebruik van gezichtsherkenningstechnologie voor biometrische authenticatie of identificatie met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen, betrekking heeft op aangelegenheden "met rechtsgevolgen in meer dan één lidstaat", omdat er, zoals toegelicht in het verzoek[5], op de luchthavens van de lidstaten momenteel verschillende projecten lopen en wordt verwacht dat daarvan de komende jaren meer gebruik zal worden gemaakt. De modellen die momenteel door verschillende luchthavens en luchtvaartmaatschappijen worden getest, verschillen aanzienlijk van lidstaat tot lidstaat. Dit kan het risico met zich meebrengen dat er, vanuit het oogpunt van gegevensbescherming, uiteenlopende gevolgen optreden in meer dan één lidstaat.

8. Bovendien is het Comité van mening dat het verzoek van de FR TA belangrijke gevolgen heeft voor de toepassing van de beginselen van artikel 5, lid 1, punten e) en f), AVG en voor de op verwerkingsverantwoordelijken van toepassing zijnde vereisten van artikel 25 AVG, evenals voor de op verwerkingsverantwoordelijken en verwerkers van toepassing zijnde vereisten van artikel 32 AVG. Dit verzoek betreft derhalve een "aangelegenheid van algemene strekking" in de zin van artikel 64, lid 2, AVG, aangezien het betrekking heeft op de consistente interpretatie van de beginselen van opslagbeperking (artikel 5, lid 1, punt e), AVG) en integriteit en vertrouwelijkheid (artikel 5, lid 1, punt f), AVG) en van de begrippen "gegevensbescherming door ontwerp en door standaardinstellingen" (artikel 25 AVG) en "gegevensbeveiliging" (artikel 32 AVG), teneinde onder meer de consistente toepassing van deze bepalingen in de EER te waarborgen.

[5] Verzoek, blz. 3.

9. Eventuele uiteenlopende standpunten van de lidstaten over de interpretatie van artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG zouden het risico vergroten dat luchthavenexploitanten en luchtvaartmaatschappijen gezichtsherkenningsprojecten op een niet-consistente manier gaan ontwikkelen. Aangezien de FR TA heeft aangetoond dat er een duidelijke behoefte is aan een consistente interpretatie van deze bepalingen met betrekking tot de gezichtsherkenningstechnologie voor biometrische authenticatie of identificatie van passagiers, om de passagiersstroom op luchthavens te stroomlijnen[6], is het Comité van mening dat het verzoek met redenen is omkleed, overeenkomstig artikel 10, lid 3, van het rvo EDPB.

10. Overeenkomstig artikel 64, lid 3, AVG mag het Comité geen advies over een aan haar voorgelegde aangelegenheid uitbrengen indien het daarover reeds een advies heeft uitgebracht[7]. De EDPB heeft nog geen antwoorden gegeven op de vragen die uit het verzoek voortvloeien. Hoewel de EDPB-richtsnoeren 3/2019 inzake videoapparatuur[8] reeds nuttige elementen bevatten over de beveiligingsmaatregelen die moeten worden toegepast op de verwerking van biometrische gegevens, wordt daarin niet op alle aspecten van de in het verzoek gestelde vragen ingegaan. Bovendien wordt in de beschikbare EDPB-richtsnoeren, waaronder de EDPB-richtsnoeren 3/2019 inzake videoapparatuur, geen specifieke leidraad gegeven over mogelijke elementen die moeten worden geverifieerd met betrekking tot de gecentraliseerde of gedecentraliseerde opslag van biometrische gegevens voor de identificatie of authenticatie van passagiers om de passagiersstroom op luchthavens te stroomlijnen, en evenmin over de verenigbaarheid van een dergelijke verwerking met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG.

11. Om deze redenen is het Comité van mening dat het verzoek ontvankelijk is en dat de vragen die erin worden gesteld, moeten worden geanalyseerd in een overeenkomstig artikel 64, lid 2, AVG vastgesteld advies.

2 TOEPASSINGSGEBIED EN CONTEXT VAN HET ADVIES

2.1 Toepassingsgebied van het advies

12. Dit advies heeft alleen betrekking op de verenigbaarheid met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG van het gebruik van gezichtsherkenningstechnologie voor de biometrische authenticatie of identificatie van passagiers door luchthavenexploitanten en luchtvaartmaatschappijen **met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen**, namelijk bij de beveiligingscontroleposten, het inchecken van bagage, het instappen en de toegang tot de passagierslounge, overeenkomstig het verzoek.

13. Wat het **toepassingsgebied van dit advies** betreft, verduidelijkt het Comité het volgende:

    1) De verwerking van persoonsgegevens in het kader van grenscontroles en door belastingvrije winkels uitgevoerde controles valt niet binnen het toepassingsgebied van dit advies, aangezien deze controles worden uitgevoerd door andere

[6] Verzoek, blz. 1-3.
[7] Artikel 64, lid 3, AVG en artikel 10, lid 4, van het reglement van orde van de EDPB.
[8] EDPB-richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, versie 2.0, vastgesteld op 29 januari 2020 (hierna "**EDPB-richtsnoeren 3/2019 inzake videoapparatuur**").

verwerkingsverantwoordelijken dan luchthavenexploitanten en luchtvaartmaatschappijen.

2) Het gebruik van gezichtsherkenningstechnologie, zelfs als dat is gebaseerd op de in deel 3.2 beschreven scenario's, voor andere doeleinden (zoals rechtshandhaving) of door andere partijen, zelfs voor vergelijkbare doeleinden, valt buiten het toepassingsgebied van dit advies.

3) Dit advies gaat alleen over de verwerking van persoonsgegevens van passagiers en heeft geen betrekking op andere soorten betrokkenen, zoals medewerkers van luchthavenexploitanten of luchtvaartmaatschappijen.

4) In dit advies wordt ingegaan op het door de FR TA ingediende verzoek met betrekking tot de verenigbaarheid van de opslagarchitecturen van de biometrische templates van de passagiers met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG. In dit opzicht bevat dit advies geen volledige en complete analyse van de naleving van de AVG door de desbetreffende verwerkingsverantwoordelijke(n) of zijn/hun eventuele verwerker(s) in elk mogelijk geval. Dit is met name belangrijk omdat deze technologieën verhoogde risico's in verband met de verwerking van de bijzondere categorieën van gegevens overeenkomstig artikel 9 AVG met zich meebrengen. Dit advies laat een beoordeling van andere bepalingen van de AVG wat betreft het gebruik van gezichtsherkenningstechnologieën, onder meer in de specifieke sector waarop het verzoek betrekking heeft, dan ook onverlet, evenals een juridische en technische analyse per geval op basis van de door een verwerkingsverantwoordelijke beoogde specifieke verwerking en de omstandigheden.

5) In dit advies wordt niet ingegaan op de verwerking van persoonsgegevens van kinderen, en het advies laat eventuele specifieke vereisten die in dat verband van toepassing zijn, onverlet.

6) Dit advies laat de wettelijke vereisten en verdere beperkingen in verband met het gebruik van biometrische gegevens die uit de nationale wetgeving van de lidstaten voortvloeien, onverlet[9].

7) Elke conclusie in dit advies laat verdere technologische ontwikkelingen onverlet.

8) In dit advies worden vier scenario's onderzocht, waarvan de specifieke kenmerken worden beschreven in deel 3.2. Het advies betreft geen andere scenario's, ook geen scenario's waarin de verwerking voor dezelfde doeleinden wordt uitgevoerd.

14. In haar verzoek heeft de FR TA aangegeven dat de verwerking van biometrische gegevens van passagiers ten behoeve van het stroomlijnen van de passagiersstroom op luchthavens zou worden gebaseerd op de veronderstelling dat de individuen toestemming geven voor een dergelijke verwerking, hetgeen mogelijk de rechtsgrondslag overeenkomstig de AVG zou vormen[10]. **De analyse van de toepasselijke <u>rechtsgrondslag valt echter niet binnen de reikwijdte</u> van de vragen die in het**

[9] In artikel 9, lid 4, AVG is bijvoorbeeld bepaald dat de lidstaten bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van biometrische gegevens kunnen handhaven of invoeren.
[10] Verzoek, bijlage I.

verzoek aan de EDPB worden voorgelegd, en bijgevolg <u>wordt de geldigheid van toestemming voor een dergelijke verwerking overeenkomstig de artikelen 6, 7 en 9 AVG in dit advies niet onderzocht</u>.

15. Niettemin merkt de EDPB in het algemeen op dat indien de desbetreffende verwerkingsverantwoordelijken zich op deze rechtsgrondslag zouden baseren, zij de geldige uitdrukkelijke toestemming zouden moeten verkrijgen[11] van de individuen die van dergelijke diensten gebruik wensen te maken. Een dergelijke uitdrukkelijke toestemming zou vrijelijk moeten worden gegeven en zou specifiek en geïnformeerd moeten zijn[12], en of aan deze voorwaarden is voldaan, zou van geval tot geval worden geanalyseerd. Dit betekent onder meer dat:

    1) individuen een dergelijke toestemming te allen tijde en zonder nadelige gevolgen gemakkelijk zouden moeten kunnen intrekken[13];

    2) om de toestemming als vrijelijk gegeven te kunnen aanmerken, een dergelijk gebruik van biometrische technologieën alleen op vrijwillige basis kan plaatsvinden, aangezien individuen vrijelijk moeten kunnen kiezen of zij al dan niet van deze diensten gebruik willen maken, en zonder nadelige gevolgen (zoals aanzienlijk langere vertragingen voor passagiers die geen toestemming geven[14]), stimulansen, extra kosten of extra voordelen als tegenprestatie[15];

    3) er ook uitdrukkelijke toestemming zou moeten worden gevraagd van individuen wier biometrische gegevens worden verwerkt, zelfs als zij zich niet hebben aangemeld voor identificatie of authenticatie met dergelijke middelen. Met andere woorden, het is van wezenlijk belang dat individuen die niet uitdrukkelijk hebben ingestemd met gezichtsherkenning voor het beoogde doel, niet aan een gezichtsscan met camera's worden onderworpen. Dit kan bijvoorbeeld worden bereikt door specifieke doorgangen voor gezichtsherkenning te reserveren en door te zorgen voor passende bewegwijzering en fysieke afscheiding van de stromen voor niet-biometrische controle om een duidelijke identificatie van deze doorgangen mogelijk te maken;

    4) ongeacht de vraag of toestemming de toepasselijke rechtsgrondslag voor een dergelijke verwerking zou vormen, de in artikel 5 AVG vastgelegde beginselen inzake verwerking met betrekking tot noodzaak en evenredigheid nog steeds van toepassing

[11] Overeenkomstig artikel 4, lid 14, en artikel 9, lid 1, en lid 2, punt a), AVG is de verwerking van biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon verboden, tenzij de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in artikel 9, lid 1, AVG genoemde verbod niet door de betrokkene kan worden opgeheven. Zie ook de overwegingen 51, 52 en 53 AVG.

[12] Artikel 4, lid 11, en artikel 7 AVG.

[13] Artikel 7, lid 4, en overweging 50 AVG.

[14] Dit kan bijvoorbeeld overwegingen omvatten zoals het ontwerpen van een systeem dat moet voorkomen dat er sociale druk wordt uitgeoefend op passagiers die geen toestemming willen geven, door te voorkomen dat hun keuze negatieve gevolgen zou hebben voor andere passagiers.

[15] EDPB-richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, versie 1.1, vastgesteld op 4 mei 2020 (hierna "**EDPB-richtsnoeren 5/2020 inzake toestemming**"), punten 46 en 48.

zijn, zelfs indien individuen hun uitdrukkelijke toestemming hebben gegeven voor het gebruik van hun biometrische gegevens[16].

16. In het verzoek is aangegeven[17] dat luchthavenexploitanten als verwerkingsverantwoordelijken zouden optreden wat betreft de verwerking bij beveiligingscontroleposten op luchthavens, terwijl luchtvaartmaatschappijen als verwerkingsverantwoordelijken zouden optreden wat betreft de verwerking bij het inchecken van bagage, het instappen en de toegang tot de passagierslounge. Het Comité merkt dan ook op dat er verschillende actoren bij de in het verzoek beschreven verwerking betrokken kunnen zijn en dat het de toepassing van de rollen van (gezamenlijke) verwerkingsverantwoordelijke en/of verwerker in de in deel 3.2 van dit advies beschreven scenario's niet heeft beoordeeld. In elk van de gevallen moeten de betrokken actoren worden geïdentificeerd en moeten hun verantwoordelijkheden duidelijk worden toegewezen, zodat aan de vereisten van de AVG wordt voldaan[18].

17. Daarnaast merkt het Comité op dat er momenteel geen uniform wettelijk vereiste in de EU is dat luchthavenexploitanten en luchtvaartmaatschappijen bij alle bovengenoemde controleposten passagiers identificeren en verifiëren dat de naam op de instapkaart van de passagier overeenkomt met de naam op zijn identiteitsdocument[19]. Dergelijke vereisten vallen dus onder de nationale wetgeving, die van lidstaat tot lidstaat kan verschillen. In sommige lidstaten kan een dergelijke verificatie worden vereist voor sommige controleposten (bv. het inchecken van bagage of het instappen), terwijl in andere lidstaten dergelijke controles thans niet worden vereist[20]. Het bestaan van wettelijke verplichtingen om de identiteit van passagiers te controleren heeft rechtstreeks gevolgen voor de praktijken op de verschillende luchthavens.

18. In deze situaties, **waarin er geen verificatie van de identiteit van de passagiers aan de hand van een officieel identiteitsdocument is vereist, hoeft er bijgevolg geen verificatie met behulp van biometrische technologie te worden uitgevoerd, aangezien dit tot een overmatige verwerking van gegevens zou leiden. Er zouden immers extra gegevens worden verwerkt vergeleken met de huidige situatie en dit zou verder gaan dan nodig is voor het desbetreffende doel, wat indruist tegen het beginsel van minimale gegevensverwerking van artikel 5, lid 1, punt c), AVG.** Een dergelijke

[16] Idem, punt 5.
[17] Verzoek, bijlage I.
[18] Overeenkomstig artikel 4, leden 7 en 8, artikel 5, lid 2, en de artikelen 24, 26, 28 en 29 AVG. Zie ook EDPB-richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, versie 2.1, vastgesteld op 7 juli 2021.
[19] De desbetreffende verordening op EU-niveau is Uitvoeringsverordening (EU) 2015/1998 van de Commissie van 5 november 2015 tot vaststelling van gedetailleerde maatregelen voor de tenuitvoerlegging van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart. Deze verordening heeft echter geen betrekking op controles van officiële identiteitsdocumenten bij controleposten op luchthavens, en de lidstaten zijn bevoegd om dit op nationaal niveau te regelen.
[20] Dit betekent dat er momenteel geen enkele controle wordt uitgevoerd of dat er alleen wordt gecontroleerd of de passagier over een instapkaart beschikt. Zo zijn burgers van Noorwegen, Denemarken, Finland en Zweden op basis van het op 22 mei 1954 tot stand gekomen protocol betreffende de vrijstelling van onderdanen van Denemarken, Finland, Noorwegen en Zweden van de verplichting om over een paspoort of verblijfsvergunning te beschikken gedurende hun verblijf in een andere dan hun eigen Noordse Staat, vanaf 1 juli 1954 vrijgesteld van de verplichting om bij het reizen tussen deze landen over een paspoort of ander reisdocument te beschikken.

beschouwing moet in aanmerking worden genomen met betrekking tot het onderzoek van alle in deel 3.2 van dit advies beschreven scenario's.

2.2 Kernbegrippen

19. Om als biometrische gegevens overeenkomstig artikel 4, lid 14, AVG te worden aangemerkt[21], moet de verwerking van ruwe gegevens, zoals de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon, gepaard gaan met een meting van deze kenmerken, aangezien biometrische gegevens het resultaat zijn van dergelijke metingen[22].

20. Aan de hand van de afbeelding van het gezicht van een persoon (foto of video), een zogenoemd biometrisch "**monster**", is het mogelijk om een digitale weergave van de onderscheidende kenmerken van dit gezicht te extraheren (dit wordt een "**template**" genoemd)[23]. Daarnaast herinnert het Comité eraan dat "[e]en biometrische template een digitale weergave [is] van de unieke kenmerken die uit een biometrisch monster zijn verkregen en in een biometrische database [kan] worden opgeslagen"[24], en dat deze unieke kenmerken de unieke identificatie van een natuurlijke persoon mogelijk maken of bevestigen. Bovendien "wordt [deze biometrische template] verondersteld voor elke persoon uniek en specifiek te zijn en blijft [de template] in beginsel constant in de loop der tijd"[25]. In een vergelijkingsproces dat is gericht op het identificeren of authenticeren van een persoon via gezichtsherkenning, wordt doorgaans een binnenkomende biometrische template vergeleken met opgeslagen objecten om een match te verifiëren of er een te vinden in een databank[26].

21. Gezichtsherkenningstechnologie kan twee verschillende functies vervullen: authenticatie[27] en identificatie[28]. Hoewel de twee functies van elkaar verschillen, zijn zij beide gebaseerd op de

---

[21] Zie ook de overwegingen 51, 52 en 53 AVG.
[22] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 74.
[23] EDPB-richtsnoeren 05/2022 voor het gebruik van gezichtsherkenningstechnologie in het kader van rechtshandhaving, versie 2.0, vastgesteld op 26 april 2023 (hierna "**EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving**"), punten 7 en 8.
[24] Idem, punt 9.
[25] Idem.
[26] EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving, punten 10 en 11; zie ook de internationale norm ISO/IEC 2382-37, 2022-03, beschikbaar op: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [laatstelijk geraadpleegd op 23 mei 2024] (hierna "**ISO/IEC 2382-37**").
[27] Het Comité merkt op dat in artikel 3, lid 36, van de komende verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) (nog niet bekendgemaakt in het *Publicatieblad van de Europese Unie*) "biometrische verificatie" ook wordt gedefinieerd als "de geautomatiseerde één-op-éénverificatie, met inbegrip van de authenticatie, van de identiteit van natuurlijke personen door hun biometrische gegevens te vergelijken met eerder verstrekte biometrische gegevens" (zie wetgevingsresolutie van het Europees Parlement van 13 maart 2024 over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie (COM(2021)0206 — C9-0146/2021 — 2021/0106(COD)).
[28] Idem, in artikel 3, lid 35, van de wet op de artificiële intelligentie wordt "biometrische identificatie" gedefinieerd als "de geautomatiseerde herkenning van fysieke, fysiologische, gedragsgerelateerde of psychologische menselijke kenmerken om de identiteit van een natuurlijk persoon vast te stellen door biometrische gegevens van die persoon te vergelijken met in een databank opgeslagen biometrische gegevens van personen".

verwerking van biometrische gegevens van een geïdentificeerde of identificeerbare natuurlijke persoon[29], en derhalve is er sprake van de verwerking van bijzondere categorieën van persoonsgegevens overeenkomstig artikel 9 AVG[30].

22. Met name:

    is **authenticatie** gericht op het bevestigen van een biometrische claim door middel van vergelijking. Dit wordt ook wel één-op-éénverificatie genoemd;

    is **identificatie** gericht op het doorzoeken van een databank met geregistreerde biometrische gegevens op identificatoren die kunnen worden toegewezen aan één enkele persoon. Dit wordt ook wel één-op-velenidentificatie genoemd.

23. In beide gevallen (d.w.z. bij identificatie en authenticatie) zijn de gezichtsherkenningstechnieken gebaseerd op een geschatte overeenstemming (match) tussen templates, d.w.z. de template die wordt vergeleken en het/de referentiepunt(en). Vanuit dit oogpunt zijn deze technieken probabilistisch: uit de vergelijking wordt met een hogere of lagere graad van waarschijnlijkheid afgeleid dat de persoon inderdaad de persoon is die moet worden geauthenticeerd of geïdentificeerd; als deze waarschijnlijkheid boven een bepaalde door de gebruiker of de ontwikkelaar van het systeem gedefinieerde drempel in het systeem komt, zal het systeem aannemen dat er een match is voor de identificatie of authenticatie[31].

[29] ISO/IEC 2382-37.
[30] Artikel 4, lid 14, AVG en EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving, punt 12.
[31] EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving, punt 11. Zie ook ISO/IEC 2382-37.

3 OVER DE GEGRONDHEID VAN HET VERZOEK

3.1 Algemene opmerkingen

24. In dit hoofdstuk worden de in punt 4 gestelde vragen geanalyseerd. Het Comité zal in dit verband voor vraag 1 de verenigbaarheid met artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG analyseren, en voor vraag 2 de verenigbaarheid met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG.

25. Het Comité zal daartoe vier verschillende scenario's analyseren[32], waarvan de specifieke kenmerken in deel 3.2 worden beschreven.

26. Om te beginnen herinnert het Comité eraan dat het gebruik van biometrische gegevens, en met name gezichtsherkenningstechnologie, verhoogde risico's voor de rechten en vrijheden van betrokkenen met zich meebrengt. In de eerste plaats betreft de verwerking in kwestie biometrische gegevens, die bijzondere bescherming genieten op grond van artikel 9 AVG. Met name brengen biometrische gegevens een onomkeerbare verandering teweeg in de relatie tussen lichaam en identiteit, doordat zij de kenmerken van het menselijk lichaam "machineleesbaar" maken en geschikt voor verder gebruik[33]. Bovendien kan het gebruik van gezichtsherkenningstechnologie risico's met zich meebrengen die verband houden met fout-negatieve resultaten, vooroordelen en discriminatie[34], en de mogelijkheid van misbruik van biometrische gegevens kan ernstige gevolgen hebben voor natuurlijke personen, zoals identiteitsfraude of impersonatie[35]. Er moet tevens op worden gewezen dat wanneer gezichtsherkenning op afstand en zonder actieve betrokkenheid van de betrokkene plaatsvindt, individuen zich mogelijk nog minder bewust zijn van een dergelijke verwerking en de bijbehorende risico's. Ten slotte is het belangrijk om te benadrukken dat de kenmerken waarop biometrische gegevens zijn gebaseerd, in het algemeen als permanent kunnen worden beschouwd en als onherroepelijk moeten worden behandeld, met name in de context van gezichtsherkenning[36].

27. Rekening houdend met het bovenstaande moeten verwerkingsverantwoordelijken derhalve, alvorens gebruik te maken van dergelijke technologieën, zelfs indien deze als bijzonder doeltreffend zouden worden beschouwd, de gevolgen voor de grondrechten en de fundamentele vrijheden van

---

[32] De vier door het Comité geanalyseerde scenario's zijn gebaseerd op gebruiksgevallen die zijn beschreven in bijlage I bij het verzoek. De FR TA heeft verduidelijkt dat de in bijlage I bij het verzoek beschreven gebruiksgevallen tot een scenario behorende voorbeelden van de uitvoering zijn die worden gebruikt ter illustratie.

[33] Advies 3/2012 van de Groep gegevensbescherming artikel 29 over ontwikkelingen op het gebied van biometrische technologieën, vastgesteld op 27 april 2012, WP193 (hierna "**Advies 3/2012 van de Groep gegevensbescherming artikel 29 over biometrische technologieën**"), blz. 4. Opgemerkt zij dat dit advies betrekking heeft op Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ("richtlijn gegevensbescherming"). In de AVG is het toepassingsgebied van de bijzondere categorieën van gegevens verruimd en, anders dan in de richtlijn gegevensbescherming, is in de AVG bepaald dat biometrische gegevens bijzondere categorieën van gegevens zijn (artikel 9 AVG).

[34] Richtsnoeren inzake gezichtsherkenning, Adviescommissie inzake het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, juni 2021, blz. 15; ook EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving, punt 27.

[35] Advies 3/2012 van de Groep gegevensbescherming artikel 29 over biometrische technologieën, blz. 29.

[36] EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving, punt 104.

betrokkenen beoordelen en moeten zij nagaan of het legitieme doel van de verwerking met minder indringende middelen kan worden bereikt[37].

28. Het Comité herinnert er tevens aan dat het recht op bescherming van persoonsgegevens geen absolute gelding heeft en conform het evenredigheidsbeginsel moet worden afgewogen tegen andere grondrechten die door het Handvest worden beschermd[38].

29. Artikel 25, lid 1, AVG heeft betrekking op "de gegevensbeschermingsbeginselen" die zijn vermeld in artikel 5 AVG[39], en daarin wordt vereist dat deze "op een doeltreffende manier" door ontwerp worden uitgevoerd[40]. Dit omvat uitdrukkelijk het beginsel van minimale gegevensverwerking van artikel 5, lid 1, punt c), AVG[41], op grond waarvan persoonsgegevens "toereikend [moeten] zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt", waarmee uitdrukking wordt gegeven aan het evenredigheidsbeginsel[42]. Daarnaast wordt in artikel 25, lid 2, AVG de verplichting tot "minimale gegevensverwerking door standaardinstellingen" verduidelijkt door de bepaling dat deze verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan[43].

30. In artikel 25 AVG wordt echter niet voorgeschreven dat verwerkingsverantwoordelijken specifieke technische en organisatorische maatregelen nemen, maar wordt in plaats daarvan vereist dat de gekozen maatregelen en waarborgen specifiek moeten zijn voor de context en de risico's voor de

---

[37] Overweging 39 AVG. Zie ook EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 73.

[38] Overweging 4 AVG. Zie in dit verband ook arrest van het Hof van Justitie van 22 juni 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (hierna "C-439/19 Latvijas Republikas Saeima"), punten 98, 110 en 113. Bovendien vereist het evenredigheidsbeginsel, als algemeen beginsel van het Unierecht, dat de maatregelen ter uitvoering van een Uniehandeling geschikt zijn om de nagestreefde doelstellingen te bereiken en niet verder gaan dan daartoe noodzakelijk is (zie arrest van het Hof van Justitie van 9 november 2010, Volker und Markus Schecke en Eifert, C-92/09 en C-93/09, ECLI:EU:C:2010:662 (hierna "C-92/09 en C-93/09 Volker und Schecke"), punt 74 en aldaar aangehaalde rechtspraak).

[39] EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, versie 2.0, vastgesteld op 20 oktober 2020 (hierna "**EDPB-richtsnoeren 4/2019 inzake gegevensbescherming door ontwerp en door standaardinstellingen**"), punt 11.

[40] In artikel 25, lid 1, AVG is het volgende bepaald: "Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen." Zie ook EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, punt 13.

[41] Dienovereenkomstig is in overweging 39 AVG vermeld dat persoonsgegevens alleen mogen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.

[42] C-439/19 Latvijas Republikas Saeima, punt 98, en arrest van het Hof van Justitie van 11 december 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 (hierna "C-708/18 M5A-ScaraA"), punt 48.

[43] EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, punt 48.

rechten en vrijheden van de betrokkene die de verwerking met zich meebrengt[44]. Evenzo wordt in artikel 32 AVG inzake beveiliging van de verwerking vereist dat verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen treffen om een op het risico voor de rechten en vrijheden van natuurlijke personen afgestemd beveiligingsniveau te waarborgen.

31. Belangrijk is dat, zelfs als passagiers uitdrukkelijk zouden instemmen met het gebruik van hun biometrische gegevens om de passagiersstroom op luchthavens te stroomlijnen, de in de AVG vastgelegde beginselen van verwerking met betrekking tot noodzaak en evenredigheid nog steeds van toepassing zijn en moeten worden nageleefd[45].

32. Wat het **noodzaakbeginsel** betreft, zal het Comité nagaan of de voorgestelde verwerking noodzakelijk is om de nagestreefde doelstelling te verwezenlijken en of dezelfde doelstelling op een even doeltreffende wijze kan worden bereikt met andere middelen die in mindere mate afbreuk doen aan de grondrechten en de fundamentele vrijheden van de betrokkene[46]. Wat het **evenredigheidsbeginsel** betreft, zal het Comité beoordelen of de negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van de betrokkenen in verhouding staan tot het eventuele verwachte voordeel. Indien het voordeel relatief gering is, staan deze gevolgen mogelijk niet in verhouding tot het verwachte voordeel[47].

33. Hoe dan ook, zelfs als het Comité van mening is dat een van de hieronder geanalyseerde scenario's aan de vereisten van artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG zou kunnen voldoen, staat het in elk geval aan de verwerkingsverantwoordelijke om dit met feitelijke elementen aan te tonen. Daarbij moet ook rekening worden gehouden met alternatieve scenario's.

3.2 Over de verenigbaarheid met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG

3.2.1 Scenario 1: opslag van de geregistreerde biometrische template alleen in handen van het individu, voor authenticatie

34. In dit hoofdstuk wordt ingegaan op de verenigbaarheid met artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG van de opslag van de biometrische template van passagiers alleen in handen van het individu, bijvoorbeeld op zijn persoonlijke apparaat[48], onder zijn uitsluitende controle[49], voor authenticatie[50] (hierna "**scenario 1**"). In dit hoofdstuk wordt ook op de passende waarborgen voor scenario 1 ingegaan in het licht van de artikelen 25 en 32 AVG.

Beschrijving van het scenario

[44] EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, punt 14.
[45] EDPB-richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/ 679, punt 5.
[46] C-439/19 Latvijas Republikas Saeima, punten 110 en 113, en arrest van het Hof van Justitie (Grote kamer) van 4 juli 2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, punt 108.
[47] C-708/18 M5A-ScaraA, punten 52-56; C-92/09 en C-93/09 Volker und Schecke, punt 87, en C-439/19 Latvijas Republikas Saeima, punten 98, 110 en 113. Zie ook Advies 3/2012 van de Groep gegevensbescherming artikel 29 over biometrische technologieën, blz. 8.
[48] Als alternatief zou het individu zijn biometrische template op papier kunnen afdrukken en opslaan.
[49] Dit laat de algehele verantwoordelijkheid van de verwerkingsverantwoordelijke voor de verwerking onverlet.
[50] Zoals geïllustreerd door gebruiksgeval 1 in bijlage I bij het verzoek.

35. In scenario 1 wordt de geregistreerde biometrische template van elke passagier die toestemming heeft gegeven voor een dergelijke verwerking alleen opgeslagen in handen van het individu, bijvoorbeeld op een persoonlijk apparaat van elke passagier, onder zijn uitsluitende controle. De passagiers worden geauthenticeerd (één-op-éénvergelijking) wanneer zij door specifieke controleposten op de luchthaven gaan.

36. De registratie wordt uitgevoerd door de luchthavenexploitant, hetzij op afstand via de app van de luchthavenexploitant[51], hetzij in de luchthaventerminals met een passend identiteitsbetrouwbaarheidsniveau (bv. passend eIDAS-betrouwbaarheidsniveau[52]). Een dergelijke registratie bestaat uit het opslaan, op het apparaat van de passagier, van een biometrische template en de identificatiegegevens[53] (hierna "**ID**") die noodzakelijk zijn voor de verwerking. De registratie vindt slechts eenmaal plaats en voor een specifieke geldigheidsperiode (bijvoorbeeld afgestemd op de geldigheidsperiode van het paspoort van de passagiers). Noch de ID van de passagiers, noch hun biometrische gegevens worden door de luchthavenexploitant na het registratieproces bewaard.

37. Met name wat de opslag betreft, worden de ID en de biometrische template van de passagier lokaal opgeslagen op het apparaat van elke passagier (bv. in de mobiele app van de luchthavenexploitant of in een app voor een digitale portemonnee). Het apparaat kan vervolgens worden gebruikt om de ID en de biometrische template van de passagiers te verzenden of op te vragen, mogelijk met inbegrip van vluchtinformatie en/of de instapkaart. Deze informatie wordt bijvoorbeeld versleuteld met een sleutel die alleen in handen is van de luchthavenexploitant — eventueel gecodeerd in de vorm van een QR-code, die op papier kan worden afgedrukt of op het beeldscherm van het apparaat van de passagier kan worden weergegeven. In dit geval zou de passagier deze QR-code vervolgens tonen aan speciale controlepods op de luchthaven, die zijn uitgerust met een QR-scanner en een camera.

38. Wat de beveiliging betreft, worden de QR-codes tijdens de matching gedecodeerd met een sleutel die in handen is van de luchthavenexploitant, die als enige de QR-codes kan decoderen. De biometrische gegevens van de passagiers worden slechts gedurende een zeer korte periode bewaard en worden na de matching gewist. Opgemerkt zij dat beveiligingsmaatregelen wat de opslag betreft gedeeltelijk afhankelijk zijn van de beveiliging van het apparaat van de passagier.

Beoordeling door de EDPB

39. In scenario 1 worden de technische en organisatorische maatregelen beschreven die een beveiligingsniveau moeten waarborgen dat is afgestemd op de risico's voor betrokkenen, zoals vereist op grond van artikel 5, lid 1, punt f), en artikel 32 AVG. De passagiers worden geauthenticeerd (één-op-éénvergelijking) wanneer zij door specifieke controleposten op de luchthaven gaan. In dit scenario

[51] De EDPB merkt op dat in de toekomst alternatieve manieren voor een dergelijke registratie kunnen worden overwogen en dat de registratie mogelijk kan worden uitgevoerd zonder een specifieke app van de luchthavenexploitant, bijvoorbeeld door middel van interactie met de digitale portemonnee van een gebruiker.
[52] Een kader voor elektronische identificatie en vertrouwensdiensten (hierna "**eIDAS**") op basis van Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit.
[53] In dit advies worden onder identificatiegegevens gegevens verstaan zoals achternaam, voornaam, geboortedatum enz. waarvan is vastgesteld dat zij juist zijn met betrekking tot een identiteitsdocument of paspoort.

wordt de belangrijkste matching uitgevoerd in de context van een gecontroleerde omgeving[54], waarin de passagiers actief betrokken zijn en meer controle over hun gegevens hebben. Met name zouden alleen passagiers worden gecontroleerd die toestemming hebben gegeven voor een dergelijke verwerking en, aangezien zij bij speciale pods zouden worden gecontroleerd, zouden de biometrische gegevens van andere passagiers die geen toestemming voor een dergelijke verwerking hebben gegeven niet worden verzameld. Daarnaast hebben de passagiers die toestemming hebben gegeven de mogelijkheid om de verwerking op elk moment stop te zetten door de gegevens van hun apparaat te verwijderen.

40. Het gebruik van gezichtsherkenning op basis van een biometrische template die alleen in handen van het individu wordt opgeslagen, bijvoorbeeld op een persoonlijk apparaat van de passagier, onder zijn uitsluitende controle, en die bij specifieke controleposten wordt gebruikt voor authenticatie door middel van een speciale interface, brengt in bepaalde omstandigheden minder risico's met zich mee dan het gebruik van biometrische gegevens waarbij de gegevens worden opgeslagen in een gecentraliseerde databank[55]. Een dergelijke gelokaliseerde opslag die gepaard gaat met passende waarborgen[56] vermindert de ernst van inbreuken in verband met persoonsgegevens in vergelijking met gecentraliseerde opslag, wat het aantal getroffen personen betreft, en zorgt ervoor dat toegang tot de biometrische template alleen mogelijk is met de actieve betrokkenheid van de betrokkene.

41. Bovendien kan de matching lokaal op de luchthaven worden uitgevoerd door de biometrische template, die bijvoorbeeld in de QR-code is opgenomen, te vergelijken met de output van de template, die is berekend op basis van het biometrische monster dat door de camera van de controlepod is genomen. Alleen het matchingresultaat zou worden bekendgemaakt aan en gebruikt door de verwerkingsverantwoordelijke die een specifieke controle uitvoert (een luchthavenexploitant of een luchtvaartmaatschappij, afhankelijk van de vraag of de controle plaatsvindt bij de beveiligingscontroleposten op de luchthaven, het inchecken van bagage, het instappen en/of de toegang tot de passagierslounge). Daarnaast vormt het feit dat de voor de matching benodigde informatie (bv. de QR-code) door het individu moet worden verstrekt een tweede factor[57], en dus een versterking van de beveiliging van de authenticatie.

42. Wat betreft de verenigbaarheid met artikel 25 AVG, en met name om te voldoen aan het vereiste van minimale gegevensverwerking, moet worden gewaarborgd dat de verwerking beantwoordt aan het noodzaakbeginsel. In scenario 1 kunnen de gekozen maatregelen worden geacht aan het noodzaakbeginsel te hebben voldaan met betrekking tot het nagestreefde doel (d.w.z. het stroomlijnen van de passagiersstroom) indien, afhankelijk van de omstandigheden van de verwerking, de verwerkingsverantwoordelijke kan aantonen dat er geen minder indringende alternatieve oplossingen zijn waarmee op even doeltreffende wijze hetzelfde doel zou kunnen worden bereikt. Mogelijk kan de verwerkingsverantwoordelijke bijvoorbeeld aantonen dat, zelfs als de passagiers hun

[54] "Ongecontroleerde omgeving" heeft betrekking op het gebruik van gezichtsherkenning voor identificatie zonder actieve betrokkenheid van de betrokkenen, waarbij de template van elke persoon die het bewaakte gebied betreedt, wordt vergeleken met de templates van een brede dwarsdoorsnede van de bevolking die in een databank zijn opgeslagen (zie EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving, punt 17).

[55] EDPB-richtsnoeren 5/2022 inzake gezichtsherkenning bij rechtshandhaving, punt 17.

[56] Zoals besproken vanaf punt 46.

[57] Dit beperkt bijvoorbeeld het risico van spoofing (het aannemen van een valse identiteit). Zie ook waarborg C.1.2.

apparaat zouden moeten laten zien, in scenario 1 de verificatie wordt versneld in vergelijking met de huidige situatie, waarin een menselijke controle plaatsvindt om na te gaan of de naam op de instapkaart overeenkomt met die op het identiteitsdocument van de passagier[58]. Dit zou met name niet kunnen worden aangetoond als er thans geen controles worden uitgevoerd om de identiteit van de passagiers te controleren op basis van hun officiële identiteitsdocument (zie in dit verband punt 18).

43. Daarnaast worden de biometrische templates door de luchthavenexploitant na de registratie niet bewaard en is de periode gedurende welke de biometrische gegevens worden bewaard door de verwerkingsverantwoordelijke die de controle uitvoert zeer kort, aangezien deze gegevens worden gewist zodra de matching is voltooid. De in scenario 1 gekozen maatregelen lijken dus de omvang van de verwerking en de opslagperiode van de persoonsgegevens te beperken.

44. Wat betreft het evenredigheidsbeginsel kan de indringendheid van een dergelijke verwerking worden gecompenseerd door de actieve betrokkenheid van de passagiers, aangezien hun biometrische gegevens alleen in hun handen zouden worden opgeslagen. Daarnaast kan de toepassing van passende maatregelen, rekening houdend met de hierboven beschreven maatregelen en ervan uitgaande dat de verwerkingsverantwoordelijke voorziet in passende waarborgen zoals vereist door de specifieke verwerking in kwestie, een beveiligingsniveau waarborgen dat is afgestemd op het risico. In dat geval kunnen de negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van de betrokkenen worden geacht in verhouding te staan tot het verwachte voordeel.

45. Rekening houdend met het bovenstaande concludeert het Comité derhalve, in antwoord op vraag 1.1, dat een dergelijke verwerking **in beginsel verenigbaar kan worden geacht met artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG, mits in passende waarborgen wordt voorzien**.

Passende waarborgen

46. In dit soort scenario is de EDPB, in antwoord op vraag 1.2, van mening dat ten minste de volgende waarborgen moeten worden geboden. Er kunnen andere dan de in dit advies beschreven waarborgen worden gebruikt om dezelfde beveiligings- en gegevensbeschermingsdoelen te verwezenlijken, die rechtmatig kunnen zijn zolang zij ervoor zorgen dat het toepasselijke wettelijke kader wordt nageleefd.

47. Opmerking: dit is een globaal en niet-limitatief overzicht van de mogelijke passende waarborgen waarin een verwerkingsverantwoordelijke moet voorzien bij een oplossing die vergelijkbaar is met scenario 1. De passendheid van de waarborgen overeenkomstig de artikelen 25 en 32 AVG moet van geval tot geval worden geanalyseerd. Alle verwerkingsverantwoordelijken zullen moeten waarborgen dat zij hun eigen gegevensbeschermingseffectbeoordeling uitvoeren[59], en voor hun specifieke oplossingen kunnen aanvullende maatregelen nodig zijn die niet in dit advies zijn opgenomen.

A. Algemeen

A.1 Gegevensbeschermingseffectbeoordeling

[58] Er kan ook worden aangevoerd dat de biometrische controle mogelijk minder gevoelig voor fouten is dan een menselijke controle.
[59] Artikel 35 AVG.

A.1.1 Een gegevensbeschermingseffectbeoordeling uitvoeren, overeenkomstig de vereisten van artikel 35 AVG, wanneer de verwerkingsverantwoordelijke van plan is een nieuwe verwerkingsactiviteit in te voeren waarbij de verwerking waarschijnlijk een hoog risico inhoudt. Dit is waarschijnlijk het geval bij scenario 1, aangezien in dit scenario op grote schaal biometrische gegevens worden verwerkt[60]. Evalueren of het passend is een gezichtsherkenningssysteem in te voeren, met inbegrip van de noodzaak en evenredigheid van het systeem met betrekking tot de nagestreefde doeleinden[61], tijdens de vroege ontwerpfase en het systeem beoordelen in alle fasen van de productontwikkeling.

A.1.2 De betrokken toezichthoudende autoriteit raadplegen als de verwerking, ondanks de door de verwerkingsverantwoordelijke genomen maatregelen ter beperking van het risico, nog steeds een hoog risico inhoudt[62].

A.2 Rechten van betrokkenen en waarborgen die door verwerkingsverantwoordelijken kunnen worden toegepast

A.2.1 Waarborgen ter voorkoming van fout-negatieve resultaten. Het risico van vertekening op basis van leeftijd, gender en ras beperken door "regelmatig te beoordelen of de algoritmen werken in overeenstemming met de doelen, waarbij de algoritmen worden aangepast om ontdekte vertekening te beperken en behoorlijkheid te waarborgen bij de verwerking"[63]. Bijvoorbeeld door menselijk toezicht en menselijke tussenkomst in te voeren om eventuele vertekening te beperken en ervoor te zorgen dat passagiers niet worden gestigmatiseerd of geprofileerd.

A.2.2 Ervoor zorgen dat elke verwerking van persoonsgegevens transparant is en dat individuen zich bewust zijn van en controle hebben over de wijze waarop hun gegevens worden verwerkt voor elke verwerkingsactiviteit[64].

A.2.3 Ervoor zorgen dat er maatregelen worden genomen om te voldoen aan het doelbindingsbeginsel, zodat de gegevens niet worden gebruikt voor andere doeleinden, zoals beveiliging of opleiding.

A.2.4 Ervoor zorgen dat er geen foto of video wordt gemaakt, zelfs als deze niet wordt vastgelegd en niet wordt verwerkt, van individuen die geen toestemming geven voor gezichtsherkenning, door passende maatregelen te nemen (zoals het gebruik van een

[60] Artikel 35, lid 3, AVG en door de Groep gegevensbescherming artikel 29 opgestelde richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, vastgesteld op 13 oktober 2017, WP248rev.01, zoals door de EDPB goedgekeurd.
[61] Artikel 35, lid 7, punt b), AVG.
[62] Artikel 36, lid 1, AVG.
[63] EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, voetnoot 60, punt 70.
[64] EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, punt 68, en overweging 7 AVG.

toereikende diepte van het veld en het opnamegebied om te voorkomen dat er beelden van andere passagiers op de achtergrond of in de buurt worden genomen, en het vormen van speciale rijen waarbij duidelijk wordt aangegeven dat deze bestemd zijn voor gezichtsherkenning).

A.2.5 Wanneer dezelfde pods worden gebruikt voor passagiers die toestemming hebben gegeven en passagiers die geen toestemming hebben gegeven voor gezichtsherkenning, of als er passagiers die geen toestemming voor gezichtsherkenning hebben gegeven in het gezichtsveld verschijnen wanneer het systeem niet wordt gebruikt, wachten op een positieve actie van een passagier die toestemming heeft gegeven alvorens te beginnen met het maken van de foto of video.

A.2.6 De betrokkene de mogelijkheid bieden om te allen tijde de gegevens in een mobiele applicatie of digitale portemonnee die zich uitsluitend in zijn handen bevinden (biometrische template[65]) te verwijderen[66].

A.2.7 Het beschikbaar stellen van bruikbare alternatieven of back-upoplossingen (d.w.z. voor passagiers die geen toestemming zouden geven voor het gebruik van hun biometrische gegevens, voor passagiers die geen gebruik zouden kunnen maken van dergelijke oplossingen, of voor passagiers die ten onrechte zijn afgewezen) om er ook voor te zorgen dat de passagiers die geen toestemming hebben gegeven, geen nadeel ondervinden[67].

A.2.8 Indien een applicatie wordt gebruikt, moet deze zorgvuldig worden ontworpen en geconfigureerd om geen onnodige gegevens te verzamelen en om te voorkomen dat met softwareontwikkelingskits van derden gegevens voor andere doeleinden worden verzameld.

A.3 Verantwoordingsplicht

A.3.1 Beoordelen of er relevante gedragscodes of certificeringsmechanismen bestaan die kunnen helpen aantonen dat de in artikel 32 AVG bedoelde maatregelen ter beveiliging van de verwerking worden nageleefd[68]. Nagaan of de maatregelen geschikt zijn voor de verwerking in kwestie. Normen[69], beste praktijken en gedragscodes die worden erkend door verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken vertegenwoordigen, kunnen van pas komen bij het vaststellen van passende maatregelen.

A.3.2 Ervoor zorgen dat er elementaire beveiligingscontroles worden uitgevoerd op het apparaat van de gebruikers om de registratiefase mogelijk te maken, hoewel de passagier zelf

[65] Verwijzingen naar de biometrische template in de waarborgen voor scenario 1 stemmen overeen met de verwijzingen naar de sleutel/het geheim in scenario 2.
[66] Er zij op gewezen dat deze waarborg alleen van toepassing is op scenario 1.
[67] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 86.
[68] Artikel 32, lid 3, AVG en EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, punt 10.
[69] Zie bijvoorbeeld ISO/IEC 2382-37.

ook een rol speelt bij de bescherming van zijn gegevens, aangezien deze op zijn apparaat zijn opgeslagen. Voorbeelden van dergelijke technische controles zijn opgenomen in deel C.2 “Infrastructuur en netwerk”.

B. Organisatorisch

B.1 Beleid en naleving

B.1.1. Ervoor zorgen dat er interne toegangscontroles plaatsvinden[70] met regels voor beheerders.

B.1.2 Wanneer de gezichtsherkenningsdienst door een van de bij de verwerking betrokken partijen kan worden verricht zonder dat er ID- of biometrische gegevens (of beide) door de andere betrokken partijen moeten worden verwerkt, verbieden dat deze gegevens via die andere partijen lopen. Een luchtvaartmaatschappij heeft bijvoorbeeld geen technische toegang tot de biometrische gegevens nodig wanneer zij gebruikmaakt van de gemeenschappelijke infrastructuur van de luchthaven, zelfs niet wanneer deze luchtvaartmaatschappij als verwerkingsverantwoordelijke voor de verwerking in het kader van de AVG optreedt.

B.1.3 Een beleid voor versleuteling en sleutelbeheer[71] definiëren, bijvoorbeeld voor de verwerking van ID- en biometrische gegevens.

B.1.4 Ervoor zorgen dat hoofdstuk V van de AVG wordt nageleefd, bijvoorbeeld door ervoor te zorgen dat bij doorgiften de regels worden nageleefd als de verwerkingsverantwoordelijke tijdens het registratieproces gebruikmaakt van een dienst op afstand in een derde land.

B.1.5 Wanneer er verwerkers worden ingezet, ervoor zorgen dat er een verwerkersovereenkomst[72] overeenkomstig artikel 28, lid 3, AVG is gesloten.

B.1.6 Ervoor zorgen dat er procedures zijn voor het beheer van het menselijke toezicht en de menselijke tussenkomst, met name voor de omgang met onterechte weigeringen en met technische problemen of problemen op het gebied van bruikbaarheid.

B.2 Opleiding en tests

B.2.1. Ervoor zorgen dat het personeel adequaat is opgeleid.

[70] EDPB-richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19, vastgesteld op 21 april 2020 (hierna “**EDPB-richtsnoeren 4/2020 inzake locatiegegevens en instrumenten voor contacttracering**”), SEC-10, blz. 16.
[71] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 89.
[72] Artikel 28, lid 3, AVG.

B.2.2 Een procedure vaststellen "voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking"[73].

B.2.3. Een procedure vaststellen om te waarborgen dat de verwerking van de biometrische template van de passagier[74] voor authenticatie technisch doeltreffend en voldoende accuraat is.

B.2.4. Ervoor zorgen dat bij de registratie en bij de controlepost verzamelde biometrische monsters van voldoende kwaliteit zijn om een betrouwbare biometrische verwerking uit te voeren.

C. Technisch

C.1 Toegang

C.1.1 Tijdens de registratiefase in waarborgen voorzien om ervoor te zorgen dat de bootstrapping/ registratie plaatsvindt met een geverifieerde identiteit. Om de beoordeling van de multifactorauthenticatie van de identiteit van de gebruikers te versterken, kunnen er bijvoorbeeld maatregelen worden getroffen die kunnen variëren van met een wachtwoord beschermde eenmalige links voor het activeren van de app tot deblokkeringsmechanismen voor het lokale apparaat.

C.1.2 Waarborgen invoeren ter voorkoming van fout-positieve resultaten, presentatie-aanvallen en fraude[75].

C.1.3 Externe toegang tot de ID- en biometrische gegevens verbieden[76].

C.1.4 Ervoor zorgen dat de verwerking lokaal wordt uitgevoerd in de fasen van de registratie, verzending en matching. Het punt van de matching moet zo dicht mogelijk bij het apparaat van het individu liggen. Om de template in het persoonlijke apparaat te kunnen matchen, is mogelijk een interactie nodig met dienstverleners buiten de luchthaven en moet mogelijk gebruik worden gemaakt van openbare netwerken, met als nadeel dat dit de beschikbaarheid beïnvloedt en dat de template in handen komt van externe entiteiten.

C.1.5 Een gebruiker authenticeren om een nieuwe vlucht toe te voegen en een nieuwe versleutelde QR-code te genereren.

[73] Artikel 32, lid 1, punt d), AVG.
[74] Verwijzingen naar de biometrische template in de waarborgen voor scenario 1 stemmen overeen met de verwijzingen naar de sleutel/het geheim in scenario 2.
[75] Verslag inzake digitale identiteit van Enisa over de gebruikmaking van het concept van self-sovereign identity (SSI) om vertrouwen op te bouwen van januari 2022.
[76] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 89.

C.1.6 Maatregelen nemen om een oplossing te bieden voor een situatie waarin een passagier geen toegang meer heeft tot zijn QR-code.

C.2 Infrastructuur en netwerk

C.2.1 Besturingssysteem up-to-date houden en authenticatie inschakelen voor toegang tot het apparaat, zodat de applicatie/digitale portemonnee onder meer de ID- en biometrische gegevens automatisch verwijdert wanneer het systeem verouderd is en een beveiligingsrisico vormt.

C.2.2 De matchingeenheden (pods) isoleren van het netwerk wanneer zij in werking zijn en alle andere maatregelen treffen die noodzakelijk zijn om de beveiliging te waarborgen.

C.2.3 Een biometrische matching uitvoeren op het apparaat van de passagier of op de pod (edge computing).

C.2.4 Oplossingen bieden om zwakke punten in de beveiliging van de persoonlijke apparaten van de passagiers aan te pakken, met inbegrip van versleuteling van (ten minste) inactieve biometrische en identiteitsgegevens.

C.2.5 Een beveiligde opslag gebruiken voor (ten minste) de biometrische gegevens die zich uitsluitend in handen van de gebruiker bevinden[77], bijvoorbeeld door gebruik te maken van een beveiligde enclave op een smartphone.

C.2.6 Beveiligingsmaatregelen nemen ter waarborging van de fysieke beveiliging van de gebouwen, waaronder de biometrische terminal op de luchthaven. Zorgen voor een hoog niveau van beveiliging voor de elementen van de architectuur die ID- en biometrische gegevens verwerken (bv. berekening, gegevensstroom, tijdelijke of langdurige opslag).

C.3 Gegevensbeveiliging en -beheer bij de identiteitscontrole van gebruikers

C.3.1 De gegevens compartimenteren tijdens de verzending en opslag in ten minste drie verschillende groepen, zoals biometrische, ID- en vluchtgegevens[78]. Ervoor zorgen dat de gegevens voldoende versleuteld zijn tussen de verzending en de opslag.

C.3.2 Technische maatregelen invoeren om te waarborgen dat alleen de gegevens die rechtmatig kunnen worden verwerkt bij specifieke controleposten, bij de controlepost worden verwerkt en geverifieerd.

[77] Verwijzingen naar de biometrische template in de waarborgen voor scenario 1 stemmen overeen met de verwijzingen naar de sleutel/het geheim in scenario 2.
[78] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 89.

C.3.3 De doeltreffendheid van de verwijdering van gegevens[79] waarborgen door middel van een beveiligde verwijderingsprocedure (bijvoorbeeld werkgeheugen, cachegeheugen, eventuele back-ups) en beoordelen wanneer de verwijdering van de gegevens moet worden geautomatiseerd. De gegevensopslagperioden moeten strikt worden gehandhaafd door middel van automatische routines, zonder dat er een aanvullende actie van het individu nodig is[80].

C.3.4 De authenticiteit en integriteit van de gegevens (bijvoorbeeld handtekening) waarborgen[81].

C.3.5 De biometrische gegevens van de passagiers op het registratiepunt en bij de controlepost slechts gedurende een zeer korte periode bewaren en de gegevens verwijderen zodra de passagier door de controlepost is gegaan.

C.3.6 Wanneer voor de registratie een applicatie wordt gebruikt, tijdens de ontwikkeling van de applicatie de normen voor de beveiliging van mobiele applicaties toepassen en beveiligingstests laten uitvoeren door een derde.

C.3.7 Ervoor zorgen dat er tijdens de registratiefase beveiligingsmaatregelen worden getroffen op de luchthaven om de vertrouwelijkheid en integriteit van de biometrische gegevens van de passagier te beschermen. Als de QR-code bijvoorbeeld door de kiosk wordt afgedrukt, mag de code niet bij de kiosk worden getoond om te voorkomen dat een kwaadwillige actor een foto neemt. In het geval van verzending over korte afstand moet de gebruiker actief bij de verzending worden betrokken en moet de verzending plaatsvinden via een kanaal waarbij een kort bereik is gewaarborgd.

C.3.8 Gegevens die zich uitsluitend in handen van het individu bevinden[82], moeten in een beveiligde opslag op het apparaat van het individu worden bewaard en eventuele zwakke punten in de besturingssystemen van het apparaat moeten worden verholpen met geschikte beveiligingspatches. In het geval van een afgedrukte QR-code moet het individu worden gewezen op de bijzonder gevoelige aard van de gegevens die in de code zijn opgenomen en wat er met de code kan worden gedaan.

C.3.9 Ervoor zorgen dat de registratie wordt uitgevoerd volgens adequate technieken voor identiteitsverificatie op afstand[83].

---

[79] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 89.

[80] EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, punt 82.

[81] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 89.

[82] Verwijzingen naar de biometrische template in de waarborgen voor scenario 1 stemmen overeen met de verwijzingen naar de sleutel/het geheim in scenario 2.

[83] Zie het verslag van Enisa over identiteitsverificatie op afstand getiteld: “Analysis of methods to carry out identity proofing remotely”, maart 2021.

3.2.2 Scenario 2: gecentraliseerde opslag van de geregistreerde biometrische template in versleutelde vorm binnen de luchthaven en met een sleutel/geheim die/dat uitsluitend in handen is van de passagiers, voor authenticatie

48. In dit hoofdstuk wordt ingegaan op de verenigbaarheid met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG van de gecentraliseerde opslag, voor authenticatie, van de geregistreerde biometrische templates van de passagiers in een gecentraliseerde databank, in versleutelde vorm en met een sleutel/geheim die/dat uitsluitend in handen is van de passagier[84] (hierna "**scenario 2**"). In dit hoofdstuk wordt ook op de passende waarborgen voor scenario 2 ingegaan in het licht van de artikelen 25 en 32 AVG.

Beschrijving van het scenario

49. In scenario 2 wordt de registratie slechts eenmaal uitgevoerd, voor een bepaalde geldigheidsperiode (bijvoorbeeld één jaar na de laatste vlucht tot de vervaldatum van het paspoort), hetzij op afstand op een passend identiteitsbetrouwbaarheidsniveau (bv. passend eIDAS-betrouwbaarheidsniveau), hetzij in een luchthaventerminal. De registratie wordt beheerd door de luchthavenexploitant en bestaat in het genereren van ID- en biometrische gegevens die worden versleuteld met een sleutel/geheim.

50. De databank wordt opgeslagen in de luchthavengebouwen, onder de controle van de luchthavenexploitant. Individuele, specifieke encryptiesleutels/geheimen worden alleen opgeslagen op het apparaat van het individu (bijvoorbeeld in de mobiele app van de luchthavenexploitant). De app kan een QR-code met de sleutel/het geheim genereren, die op papier kan worden afgedrukt of op het beeldscherm van het apparaat kan worden weergegeven[85]. Daarnaast wordt door de luchthavenexploitant een tweede encryptielaag[86] toegevoegd met sleutels die worden beheerd door de luchthavenexploitant.

51. Passagiers worden geauthenticeerd (één-op-éénvergelijking) wanneer zij door specifieke controleposten op de luchthaven gaan. De passagiers die ervoor kiezen om door de biometrische controleposten te gaan, tonen hun QR-code aan een speciale controlepod die is uitgerust met een QR-scanner en een camera. De index van de passagier wordt naar de databank gezonden om de versleutelde template op te vragen, die lokaal wordt gedownload en gecontroleerd op de pod en/of het apparaat van de gebruiker. Alleen het matchingresultaat is bekend bij en wordt gebruikt door de verwerkingsverantwoordelijke van de controlepost[87].

52. In dit scenario zijn er geen stromen van ID- en biometrische gegevens tussen luchthavens en is er geen sprake van interconnectie, noch van interoperabiliteit tussen de gecentraliseerde databanken.

---

[84] Zoals geïllustreerd door gebruiksgeval 2 in bijlage I bij het verzoek.

[85] De FR TA heeft verder verduidelijkt dat er mogelijk ook andere technische oplossingen zijn voor het verzenden van de vereiste informatie, bijvoorbeeld door gebruik te maken van een protocol voor korteafstandscommunicatie.

[86] De sleutel/het geheim (in handen van het individu) is zelf versleuteld met een andere sleutel die in handen is van de luchthavenexploitant.

[87] De FR TA heeft verduidelijkt dat deze opslagperiode illustratief is en als aanvaardbaar kan worden beschouwd, aangezien de sleutel in handen is van de individuen en kan worden gekozen in de registratiefase. Er zij echter op gewezen dat de opslagperiode kan worden aangepast.

Beoordeling door de EDPB

53. In scenario 2 worden de geregistreerde biometrische templates van de passagiers gecentraliseerd opgeslagen, maar in versleutelde vorm en met een sleutel/geheim die/dat uitsluitend in handen is van de passagiers. In scenario 2 worden de passagiers geauthenticeerd (één-op-éénvergelijking).

54. In dit scenario wordt voorgesteld dat het doel van het stroomlijnen van de passagiersstroom (d.w.z. door de controle te versnellen) kan worden bereikt met behulp van een gecentraliseerd systeem. De EDPB heeft reeds opgemerkt dat een dergelijke oplossing kan worden beschouwd als een goed alternatief voor gedecentraliseerde opslag van de geregistreerde biometrische templates[88] (zoals beschreven in scenario 1), indien er een objectieve behoefte bestaat en met behulp van passende waarborgen (zie de vanaf punt 60 beschreven waarborgen).

55. Wat de beveiligingsoverwegingen betreft, worden de gegevens van elk individu versleuteld met de specifieke sleutel die alleen in het bezit is van het individu en die onder zijn uitsluitende controle valt. Bovendien vormt het feit dat de voor de matching benodigde informatie (d.w.z. het geheim/de sleutel) door het individu moet worden verstrekt een tweede factor[89], en dus een versterking van de beveiliging van de authenticatie. Daarnaast wordt door de luchthavenexploitant een tweede encryptielaag toegevoegd met sleutels die worden beheerd door de luchthavenexploitant. In scenario 2 wordt de index van het individu naar de centrale databank gezonden om de biometrische gegevens van het individu op te vragen. Deze gegevens worden vervolgens (in versleutelde vorm) verzonden naar een computer bij de controlepost, waar de gegevens worden gedecodeerd om de matching uit te voeren, en alleen het matchingresultaat is bekend bij en wordt gebruikt door de verwerkingsverantwoordelijke van de controlepost. Mits de sleutel/het geheim van het individu in de computer bij de controlepost wordt bewaard en alleen de index van een passagier naar de centrale databank wordt verzonden om de versleutelde biometrische template op te halen, kunnen de beveiligingsmaatregelen derhalve worden geacht verenigbaar te zijn met artikel 5, lid 1, punt f), en artikel 32 AVG.

56. Wat betreft de verenigbaarheid met artikel 25 AVG, en met name om te voldoen aan het vereiste van minimale gegevensverwerking, moet worden gewaarborgd dat de verwerking beantwoordt aan het noodzaakbeginsel. In scenario 2 kunnen de gekozen maatregelen worden geacht aan het noodzaakbeginsel te hebben voldaan met betrekking tot het nagestreefde doel (d.w.z. het stroomlijnen van de passagiersstroom op luchthavens) indien, afhankelijk van de omstandigheden van de verwerking, de verwerkingsverantwoordelijke kan aantonen dat er geen minder indringende alternatieve oplossingen zijn waarmee op even doeltreffende wijze hetzelfde doel zou kunnen worden bereikt. In scenario 2 zouden de passagiers nog steeds hun apparaat moeten laten zien[90]. Niettemin kan de verwerkingsverantwoordelijke mogelijk aantonen dat in scenario 2 de verificatie wordt versneld in vergelijking met de huidige situatie, waarin een menselijke controle plaatsvindt om na te gaan of de naam op de instapkaart overeenkomt met die op het identiteitsdocument van de

[88] EDPB-richtsnoeren 3/2019 inzake videoapparatuur, punt 88.

[89] Dit beperkt bijvoorbeeld het risico van spoofing (het aannemen van een valse identiteit). Zie ook waarborg C.1.2.

[90] De FR TA heeft verder verduidelijkt dat er mogelijk ook andere opties zijn om een template te laten zien, bijvoorbeeld afgedrukt op papier. Daarnaast erkent de EDPB dat in de toekomst kan worden overwogen om gebruik te maken van een alternatieve technologie, bijvoorbeeld op basis van een systeem voor contactloze korteafstandscommunicatie (near field communication).

passagier[91], of in vergelijking met scenario 1. Dit zou met name niet kunnen worden aangetoond als er thans geen controles worden uitgevoerd om de identiteit van de passagiers te controleren op basis van hun officiële identiteitsdocument (zie in dit verband punt 18).

57. Wat betreft het evenredigheidsbeginsel kan de indringendheid van een dergelijke verwerking worden gecompenseerd door de actieve betrokkenheid van de passagiers, die de sleutel tot hun versleutelde gegevens onder hun uitsluitende controle houden. Bovendien lijken de beveiligingsrisico's die zijn verbonden aan de opslag van de biometrische gegevens van de passagiers in een gecentraliseerde databank en met de sleutel uitsluitend in handen van de passagiers, te kunnen worden beperkt met behulp van passende waarborgen (zie de vanaf punt 60 besproken waarborgen). Ervan uitgaande dat de verwerkingsverantwoordelijke passende waarborgen invoert zoals vereist door de specifieke verwerking in kwestie, kunnen de risico's voor individuen derhalve worden beperkt en kunnen de negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van de betrokkenen als evenredig aan het verwachte voordeel worden beschouwd. Vanzelfsprekend moet steeds worden gewaarborgd dat alleen de voor het doel benodigde gegevens worden verwerkt en dat alleen passagiers die toestemming hebben gegeven zouden worden gecontroleerd, zodat er geen risico is dat er biometrische gegevens van andere passagiers, die geen toestemming hebben gegeven, zouden worden verzameld.

58. In het verzoek staat bijvoorbeeld dat in scenario 2 de opslagperiode van de versleutelde gegevens in de databank gewoonlijk één jaar na de laatste vlucht van het individu zou kunnen bedragen, tot de vervaldatum van het paspoort. In het verzoek is geen informatie verstrekt ter onderbouwing van een dergelijke lange periode op grond van objectieve redenen, al kan worden aangenomen dat een dergelijke opslagperiode wordt beoogd om meer gemak te bieden bij toekomstige vluchten. Wat de opslagperiode betreft, moeten de verwerkingsverantwoordelijken met het oog op de verenigbaarheid met artikel 5, lid 1, punt e), AVG in dit scenario kunnen rechtvaardigen waarom deze bewaartermijn in specifieke gevallen noodzakelijk is voor het doel van de verwerking. Het Comité beveelt de verwerkingsverantwoordelijken aan om te streven naar de kortst mogelijke opslagperiode, waarbij tevens rekening wordt gehouden met passagiers die slechts zeer zelden vliegen, en om de betrokkenen de mogelijkheid te bieden de opslagperiode van hun voorkeur in te stellen.

59. In het licht van deze overwegingen concludeert het Comité, in antwoord op vraag 2.1.1, dat een dergelijke verwerking **in beginsel verenigbaar kan worden geacht met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG, mits in passende waarborgen wordt voorzien**.

Passende waarborgen

60. In dit soort scenario is het Comité, in antwoord op vraag 2.1.2, van mening dat, **naast de in scenario 1 vermelde waarborgen**, ten minste de volgende waarborgen moeten worden geboden. Er kunnen andere dan de in dit advies beschreven waarborgen worden gebruikt om dezelfde beveiligings- en gegevensbeschermingsdoelen te verwezenlijken, die rechtmatig kunnen zijn zolang zij ervoor zorgen dat de toepasselijke wettelijke kaders worden nageleefd.

61. Opmerking: *dit is een globaal en niet-limitatief overzicht van de mogelijke passende waarborgen waarin een verwerkingsverantwoordelijke zou kunnen voorzien bij een oplossing die vergelijkbaar is*

[91] Er kan ook worden aangevoerd dat de biometrische controle mogelijk minder gevoelig voor fouten is dan een menselijke controle.

met scenario 2. De passendheid van de waarborgen overeenkomstig de artikelen 25 en 32 AVG moet van geval tot geval worden geanalyseerd. Alle verwerkingsverantwoordelijken zullen moeten waarborgen dat zij hun eigen gegevensbeschermingseffectbeoordeling uitvoeren, en voor hun specifieke oplossingen kunnen aanvullende maatregelen nodig zijn die niet in dit advies zijn opgenomen.

D. Algemeen

D.1 Rechten van betrokkenen en waarborgen die door verwerkingsverantwoordelijken kunnen worden toegepast

D.1.1 Ervoor zorgen dat de passagier voor al zijn gegevens de controle heeft over de gegevensopslagperioden. De opslagperioden moeten beperkt blijven tot wat noodzakelijk is voor het specifieke doel. Er moet een maximumperiode worden vastgesteld op basis van een grondige analyse van factoren zoals de geldigheid van het identificatiedocument. De betrokkenen moet de mogelijkheid worden geboden de opslagperiode van hun voorkeur in te stellen, die korter kan zijn dan de standaardopslagperiode.

D.1.2 De betrokkene de mogelijkheid bieden om te allen tijde te verzoeken om verwijdering van de gegevens in een mobiele applicatie of digitale portemonnee die zich uitsluitend in zijn handen bevinden (sleutel/geheim)[92].

D.1.3 Ervoor zorgen dat de locatie van de centrale databank een doeltreffend toezicht door de bevoegde toezichthoudende autoriteit mogelijk maakt.

E. Organisatorisch

E.1 Beleid en naleving

E.1.1 Het vertrouwen in de centrale server moet beperkt zijn. Ervoor zorgen dat bij het beheer van de centrale server duidelijk omschreven governanceregels worden gevolgd en alle maatregelen worden genomen die nodig zijn om de server te beveiligen[93].

F. Technisch

F.1 Toegang

F.1.1 Logbestanden bijhouden van wie toegang heeft tot persoonsgegevens, met name ID- en biometrische gegevens, en wanneer toegang tot de gegevens is verkregen.

F.2 Infrastructuur en netwerk

[92] Er zij op gewezen dat deze waarborg alleen van toepassing is op scenario 2.
[93] EDPB-richtsnoeren 4/2020 inzake locatiegegevens en instrumenten voor contacttracering, PRIV-5, blz. 17.

F.2.1 Zorgen voor een passende beveiliging van de centrale databank, tegen onder meer beschikbaarheidsaanvallen.

F.2.2 Ervoor zorgen dat er geen internetverbinding is met de centrale databank, de registratiepods en de matchingeenheden. De bediening en het onderhoud van deze systemen (bv. back-up, patching, monitoring enz.) moeten op lokaal niveau worden uitgevoerd binnen de luchthavengebouwen.

F.3 Gegevensbeveiliging en -beheer

F.3.1 Geavanceerde cryptografische technieken toepassen om de communicatie tussen de applicatie en de gecentraliseerde server te beveiligen[94].

F.3.2 De individuele sleutel/het individuele geheim op het niveau bewaren waarop deze/dit zal worden gebruikt voor decodering (d.w.z. in de pod) en de index alleen gebruiken om de bijbehorende geregistreerde biometrische template in de centrale databank op te halen.

F.3.3 Ervoor zorgen dat de uitwisseling van de sleutel/het geheim tussen het apparaat van de gebruiker en de pod de communicatie beschermt tegen mogelijk afluisteren of overdracht aan derden.

F.3.4 De biometrische template indexeren wanneer deze is opgeslagen in de centrale databank om één-op-éénauthenticatie mogelijk te maken, en ervoor zorgen dat deze template uniek is en gerelateerd is aan het individu. Ervoor zorgen dat de index geen identiteitsinformatie van de passagier onthult en niet gecorreleerd is met de encryptiesleutel.

F.3.5 Zorgen voor een passende authenticatie en de overdracht tussen de centrale databank en de controleposten versleutelen, en daarvoor geïsoleerde netwerken gebruiken.

F.3.6 Bidirectionele links tussen reeksen gegevens vermijden (ID- en biometrische gegevens, evenals vluchtgegevens) en alleen relevante unidirectionele links in de databank bewaren. Bijvoorbeeld alleen de unidirectionele links van index naar ID, van index naar versleutelde biometrische gegevens, en van index naar vluchtgegevens.

F.3.7 Ervoor zorgen dat er regelingen zijn ter verzekering van de continuïteit van de bedrijfsuitoefening, bijvoorbeeld door passende back-upsystemen te installeren.

---

[94] EDPB-richtsnoeren 4/2020 inzake locatiegegevens en instrumenten voor contacttracering, SEC-4, blz. 16: "Hiervoor kunnen onder meer de volgende technieken worden gebruikt: symmetrische en asymmetrische encryptie, hashfuncties, PMT (private membership test), PSI (private set intersection), bloomfilters, PIR (private information retrieval), homomorfe encryptie enz."

F.3.8 Ervoor zorgen dat in de pod geen logbestanden worden bijgehouden van de versleutelde of niet-versleutelde templates.

3.2.3 Gecentraliseerde opslag van de geregistreerde biometrische templates voor identificatie

62. In dit hoofdstuk wordt ingegaan op de verenigbaarheid met artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG van de gecentraliseerde opslag, voor identificatie, van de geregistreerde biometrische templates van de passagiers, wanneer deze templates niet zijn versleuteld met een sleutel/geheim die/dat uitsluitend in handen is van de passagiers, in twee gebruiksgevallen: 1) wanneer deze templates worden opgeslagen in een databank binnen de luchthaven, onder de controle van de luchthavenexploitant[95] (hierna "**scenario 3.1**"), en 2) wanneer deze templates worden opgeslagen in de cloud, onder de controle van de luchtvaartmaatschappij[96] (hierna "**scenario 3.2**").

63. Het Comité is van mening dat het gebruik van biometrische gegevens voor **identificatiedoeleinden** in grote centrale databanken de grondrechten van betrokkenen aantast en mogelijk ernstige gevolgen voor de betrokkenen kan hebben[97]. Daarnaast moet het gebruik van biometrische gegevens ook worden onderzocht in relatie tot het doel waarvoor deze gegevens worden verwerkt, in het licht van de noodzaak- en evenredigheidsbeginselen[98].

3.2.3.1 Scenario 3.1: gecentraliseerde opslag in een databank binnen de luchthaven, onder de controle van de luchthavenexploitant

Beschrijving van het scenario

64. In scenario 3.1 wordt de geregistreerde biometrische template van de passagiers in versleutelde vorm opgeslagen in een centrale databank in de luchthavengebouwen en onder de controle van de luchthavenexploitant. Met name worden de gegevens van de passagiers gecompartimenteerd, wat inhoudt dat hun identiteitsgegevens, hun geregistreerde biometrische template en hun vluchtinformatie worden opgeslagen in drie verschillende databanken. Deze gegevens worden versleuteld met verschillende sleutels, zowel tijdens de opslag als tijdens de verzending naar de servers die de matching uitvoeren, waar de gegevens vervolgens worden gedecodeerd door de luchthavenexploitant.

65. De passagiers moeten zich voor elke vlucht registreren, kort voor hun vertrek (bv. 48 uur). Een dergelijke registratie kan ofwel op afstand ofwel in een luchthaventerminal worden uitgevoerd op een passend identiteitsbetrouwbaarheidsniveau (bv. passend eIDAS-betrouwbaarheidsniveau). Bij wijze van alternatief kan de registratie dezelfde vorm aannemen als beschreven in scenario 1, in welk geval de passagiers binnen 48 uur voorafgaand aan hun vertrek hun gegevens van hun digitale portemonnee naar het luchthavensysteem moeten sturen.

---

[95] Zoals geïllustreerd door gebruiksgeval 3A in bijlage I bij het verzoek.
[96] Zoals geïllustreerd door gebruiksgeval 3B in bijlage I bij het verzoek.
[97] Zie bijvoorbeeld Advies 3/2012 van de Groep gegevensbescherming artikel 29 over biometrische technologieën, blz. 8. Zie ook punt 26.
[98] Overweging 4 AVG. Zie ook Advies 3/2012 van de Groep gegevensbescherming artikel 29 over biometrische technologieën, blz. 8.

66. Ook in dit scenario melden de passagiers zich bij een speciale controlepod die is uitgerust met een camera. Hun biometrische monster wordt vervolgens naar een centrale luchthavenserver verzonden, die de gegevens aan die van de centrale biometrische databank zal proberen te koppelen. De passagier kan dus worden geïdentificeerd en er kan worden gecontroleerd of hij inderdaad is geregistreerd voor een vertrekkende vlucht (of de vlucht waarvoor wordt ingestapt in het geval van controle bij het instappen). Afhankelijk van de controlepost, kunnen de naar de verzoekende verwerkingsverantwoordelijke van de controlepost teruggezonden gegevens tot een minimum worden beperkt, bijvoorbeeld als een "ja/nee-antwoord" of het matchingresultaat zelf, indien dit nodig is. In dit geval wordt alleen het resultaat van het verzoek doorgegeven aan en gebruikt door een verwerkingsverantwoordelijke van de controlepost.

67. Met name worden in dit scenario de passagiers geïdentificeerd (één-op-n-vergelijking), waarbij n het aantal passagiers is dat binnen een tijdsbestek van enkele dagen op de luchthaven wordt verwacht. Bovendien wordt de biometrische matching alleen uitgevoerd wanneer elke passagier zich meldt bij vooraf vastgestelde controleposten op de luchthaven van vertrek, maar vindt de gegevensverwerking zelf plaats op een centrale server die is verbonden met de centrale databank. De opslagperiode in dit scenario bedraagt doorgaans 48 uur en de gegevens worden gewist zodra het vliegtuig is vertrokken.

Beoordeling door de EDPB

68. Zoals hierboven is opgemerkt, brengt de verwerking van biometrische gegevens verhoogde risico's voor de rechten en vrijheden van betrokkenen met zich mee[99]. Elke inbreuk op de gegevensbeveiliging kan dan ook bijzonder ernstige gevolgen voor betrokkenen hebben[100]. Verwerkingsverantwoordelijken zijn verplicht om deze risico's doeltreffend te beperken. Aangezien in dit scenario de gehele architectuur volledig is gecentraliseerd, verliezen de passagiers in grotere mate de controle over hun gegevens. Bovendien kan ook het risico groter zijn dat de gegevens uiteindelijk worden verwerkt voor andere doeleinden dan het beheersen van de passagiersstroom.

69. In het licht van het beginsel en de vereisten met betrekking tot beveiliging (artikel 5, lid 1, punt f), en artikel 32 AVG) moet worden opgemerkt dat de opslag van ID- en biometrische gegevens in centrale, zij het afzonderlijke, databanken hoogwaardige aanvalspunten kan bieden en dat een inbreuk op de vertrouwelijkheid van deze databanken er vervolgens toe kan leiden dat toegang tot de gehele gegevensreeks wordt verkregen. Als gevolg daarvan kan een mogelijke inbreuk met betrekking tot gezichtsherkenningstemplates en de bijbehorende ID de ongeoorloofde of onrechtmatige identificatie van de betrokkenen in andere omgevingen mogelijk maken. Een dergelijke inbreuk kan, afhankelijk van de methoden die voor de biometrische identificatie worden gebruikt, ook het verdere veilige gebruik van gezichtsherkenningstemplates als identificatiemiddel in gevaar brengen. In dat geval kunnen de gevolgen van de inbreuk niet worden beperkt, anders dan bij een ander soort inloggegevens (bv. gebruikersnaam, wachtwoord), waarbij de gegevens kunnen worden gewijzigd[101].

[99] Zie punt 26.

[100] Richtsnoeren inzake gezichtsherkenning, Adviescommissie inzake het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, juni 2021, blz. 22.

[101] Zie in dit verband Advies 3/2012 van de Groep gegevensbescherming artikel 29 over biometrische technologieën, blz. 34.

70. Daarnaast maakt de hoge kwantiteit en kwaliteit van de ID- en biometrische gegevens bij de verwerkingsverantwoordelijke deze gegevens tot een zeer waardevol doelwit voor een aanvaller, waardoor de beveiligingsrisico's toenemen. Bovendien kunnen inbreuken in verband met persoonsgegevens grotere gevolgen hebben, aangezien het door de opslag van gegevens op een centrale locatie voor aanvallers gemakkelijker kan zijn om toegang te krijgen tot persoonsgegevens van meerdere passagiers. Een mogelijke inbreuk zou dan ook een groot aantal betrokkenen aan grote risico's kunnen blootstellen wat de ernst betreft, bijvoorbeeld identiteitsdiefstal op grote schaal, die extreem moeilijk te beperken zijn.

71. Wat betreft de verenigbaarheid met artikel 5, lid 1, punt f), en artikel 32 AVG zijn de in scenario 3.1 beoogde maatregelen[102], rekening houdend met de stand van de techniek, derhalve ontoereikend om een op het risico afgestemd beveiligingsniveau te waarborgen. Op grond van het bovenstaande zou de verwerking in scenario 3.1 niet voldoen aan artikel 5, lid 1, punt f), en artikel 32 AVG indien een verwerkingsverantwoordelijke zich tot deze maatregelen zou beperken.

72. In het licht van het beginsel van artikel 5, lid 1, punt e), AVG bedraagt de opslagperiode van biometrische gegevens in de centrale databank doorgaans 48 uur. Een dergelijke opslagbeperking lijkt de aan inbreuken in verband met persoonsgegevens verbonden risico's aanzienlijk te beperken. Niettemin is de gegevensopslagperiode op zich geen doorslaggevende factor voor de algemene verenigbaarheid van de betrokken architectuur, aangezien een dergelijke bewaarperiode door de verwerkingsverantwoordelijken kan worden gewijzigd. In elk geval moeten de voorgestelde maatregelen voldoen aan de vereisten inzake gegevensbescherming door ontwerp en door standaardinstellingen overeenkomstig artikel 25 AVG.

73. In tegenstelling tot de scenario's 1 en 2, waarin de passagiers worden geauthenticeerd, worden de passagiers in scenario 3.1 geïdentificeerd (één-op-n-vergelijking). Daarbij is n het aantal binnen een tijdsbestek van enkele dagen op de luchthaven verwachte passagiers die toestemming hebben gegeven voor een dergelijke verwerking wanneer zij door specifieke controleposten op de luchthaven gaan. Dit houdt in dat in een centrale databank naar passagiers wordt gezocht door elk vastgelegd biometrisch monster te verwerken om te controleren of het overeenkomt met een persoon die bekend is bij het systeem. In tegenstelling tot scenario 2 zijn in scenario 3.1 de sleutels niet uitsluitend in handen van de passagiers. Bijgevolg hebben de passagiers in dit scenario aanzienlijk minder controle over hun biometrische gegevens. Een verwerking zoals voorgesteld in scenario 3.1 kan dan ook niet verenigbaar zijn met de vereisten inzake gegevensbescherming door ontwerp en door standaardinstellingen overeenkomstig artikel 25 AVG.

74. In het licht van artikel 25 AVG moeten verwerkingsverantwoordelijken rekening houden met de soorten, de categorieën en de gedetailleerdheid van persoonsgegevens die nodig zijn voor de verwerkingsdoeleinden[103]. Bij hun ontwerpkeuzes moet rekening worden gehouden met de toegenomen risico's voor de beginselen van minimale gegevensverwerking, integriteit en vertrouwelijkheid, en opslagbeperking wanneer grote hoeveelheden gedetailleerde persoonsgegevens worden verzameld en moeten deze risico's worden afgezet tegen de vermindering van de risico's wanneer kleinere hoeveelheden en/of minder gedetailleerde informatie over de

[102] Zoals beschreven in de punten 64-67.

[103] EDPB-richtsnoeren 4/2019 inzake gegevensbescherming door ontwerp en door standaardinstellingen, punt 49.

betrokkenen worden verzameld. In elk geval mag de standaardinstelling er niet toe leiden dat persoonsgegevens worden verzameld die niet noodzakelijk zijn voor het specifieke verwerkingsdoeleinde. Met andere woorden, indien bepaalde categorieën van persoonsgegevens niet nodig zijn of indien er geen gedetailleerde gegevens nodig zijn omdat minder gedetailleerde gegevens voldoende zijn, mogen er geen overbodige persoonsgegevens worden verzameld. In dit geval is het niet nodig om gezichtsherkenningstechnologie te gebruiken als met een andere verwerkingsuitvoering hetzelfde doel kan worden bereikt en als deze uitvoering beschikbaar is onder de in scenario 3.1 beschreven voorwaarden.

75. Wat artikel 25 AVG betreft, is de autonomie van de betrokkene een belangrijk element van gegevensbescherming door ontwerp en door standaardinstellingen. Met name moet de betrokkene de hoogst mogelijke mate van autonomie krijgen om te bepalen hoe zijn persoonsgegevens worden gebruikt of verwerkt, en in welke mate en onder welke voorwaarden dat gebeurt[104]. In scenario 1 zou de betrokkene autonomie en controle hebben met betrekking tot het gebruik, de verstrekking en de vernietiging van zijn biometrische templates, en in scenario 2 zou de betrokkene enige controle over de verstrekking van zijn eigen biometrische template behouden, aangezien de encryptiesleutel/het geheim in zijn handen zou worden opgeslagen. In scenario 3.1 is de betrokkene echter volledig afhankelijk van de keuzes van de verwerkingsverantwoordelijke met betrekking tot de verwerking van zijn biometrische gegevens en heeft hij derhalve geen directe controle over het gebruik van zijn biometrische template.

76. Wat betreft de verenigbaarheid met artikel 25 AVG, en met name om te voldoen aan het vereiste van minimale gegevensverwerking, kan de in scenario 3.1 beoogde verwerking niet beantwoorden aan het noodzaakbeginsel. Het Comité is van mening dat een soortgelijk resultaat om de passagiersstroom op luchthavens te stroomlijnen kan worden behaald op een manier waarbij minder inbreuk op de privacy wordt gemaakt. Dit kan bijvoorbeeld worden bereikt zonder dat er biometrische gegevens worden gebruikt (hoewel de gebruikerservaring in dat geval anders zou zijn, aangezien het tonen van de instapkaart en, waar nodig, de officiële identificatiedocumenten dan meer tijd in beslag zou kunnen nemen). Bovendien kunnen met andere oplossingen, met name die welke zijn gebaseerd op de opslag van de biometrische gegevens in een lokale portemonnee op het apparaat van het individu of oplossingen waarbij de gegevens moeten worden versleuteld met een specifieke sleutel die wordt opgeslagen op het apparaat van het individu, de doelstellingen worden bereikt op een manier waarbij minder inbreuk op de privacy wordt gemaakt.

77. Wat het evenredigheidsbeginsel betreft, zou de in scenario 3.1 beoogde verwerking risico's voor de rechten van de betrokkenen met zich meebrengen die door de beoogde maatregelen niet zouden worden beperkt, gezien de stand van de techniek. Het risico van negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van betrokkenen die zouden kunnen voortvloeien uit een inbreuk in verband met persoonsgegevens in een gecentraliseerde databank met biometrische gegevens van een groot aantal personen, lijkt zwaarder te wegen dan het verwachte voordeel dat uit de verwerking voortvloeit, aangezien een dergelijk voordeel relatief gering is, d.w.z. een lichte toename van het gemak en de snelheid van de controles. Dit voordeel kan dan ook geen rechtvaardiging vormen voor de grote indringendheid van die maatregelen met betrekking tot de

[104] EDPB-richtsnoeren 4/2019 inzake gegevensbescherming door ontwerp en door standaardinstellingen, punt 70. In overweging 7 AVG wordt verder verduidelijkt dat "[n]atuurlijke personen controle over hun eigen persoonsgegevens [moeten] hebben".

grondrechten en de fundamentele vrijheden van natuurlijke personen, en de in scenario 3.1 beoogde verwerking voldoet niet aan het evenredigheidsbeginsel.

78. In het licht van deze overwegingen concludeert het Comité, in antwoord op vraag 2.2.1, dat, indien de verwerking plaatsvindt met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen, de in scenario 3.1 beoogde verwerking:

- **niet verenigbaar kan zijn met artikel 25 AVG**;
- **niet zou voldoen aan artikel 5, lid 1, punt f), en artikel 32 AVG** indien een verwerkingsverantwoordelijke zich zou beperken tot de in scenario 3.1 beschreven maatregelen.

3.2.3.2 Scenario 3.2: gecentraliseerde opslag in de cloud, onder de controle van de luchtvaartmaatschappij

Beschrijving van het scenario

79. In scenario 3.2 wordt de geregistreerde biometrische template van de passagiers opgeslagen in de cloud, onder de controle van de luchtvaartmaatschappij of haar cloudaanbieder (gegevensverwerker). In het verzoek is vermeld dat de cloudaanbieder in de EER zou zijn gevestigd[105]. In dit geval worden de gegevens van de passagiers versleuteld, maar tijdens het gebruik (bijvoorbeeld wanneer de matching wordt uitgevoerd) gedecodeerd, en worden de sleutels beheerd door de luchtvaartmaatschappij of haar cloudverwerker. De biometrische gegevens van de passagiers worden gebruikt voor de identificatie van de passagiers (één-op-n-vergelijking), waarbij n maximaal het totale aantal klanten van de luchtvaartmaatschappij is[106].

80. Net als in de scenario's 1, 2 en 3.1 moeten de passagiers zich ook hier eerst registreren. In scenario 3.2 blijven de passagiers na hun eenmalige registratie echter geregistreerd zolang zij een account aanhouden bij de luchtvaartmaatschappij. De registratie vindt hetzij op afstand plaats op een passend identiteitsbetrouwbaarheidsniveau (bv. passend eIDAS-betrouwbaarheidsniveau), hetzij in een luchthaventerminal. De biometrische matching wordt alleen uitgevoerd wanneer de passagiers zich melden bij vooraf vastgestelde controleposten op de luchthaven, maar de gegevensverwerking zelf vindt plaats in de cloud.

81. Op de luchthaven gaan de passagiers door speciale controlepods, die zijn uitgerust met een camera. De biometrische gegevens van de passagiers worden door middel van een verzoek naar een cloudserver van de luchtvaartmaatschappij verzonden, waar deze gegevens worden gematcht met de centrale databank. De passagier kan dus worden geïdentificeerd en er kan worden gecontroleerd of hij inderdaad is geregistreerd voor een vertrekkende vlucht (of de vlucht waarvoor wordt ingestapt in het geval van controle bij het instappen).

82. De matchingresultaten kunnen eventueel aan meerdere luchthavenexploitanten ter beschikking worden gesteld wanneer een luchtvaartmaatschappij over een speciale terminal beschikt of toegang heeft tot de gemeenschappelijke infrastructuur voor de informatiesystemen van een luchthaven. Afhankelijk van de controlepost, kunnen de naar de verzoekende verwerkingsverantwoordelijke van de controlepost teruggezonden gegevens tot een minimum worden beperkt, bijvoorbeeld als een "ja/nee-antwoord" of het matchingresultaat zelf, indien dit nodig is. In dit geval is alleen het resultaat van het verzoek bekend bij en wordt alleen dit resultaat gebruikt door de verwerkingsverantwoordelijke van de controlepost.

83. De opslagperiode van de template wordt vastgesteld door de luchtvaartmaatschappij en kan zo lang zijn als de klant een account heeft bij de luchtvaartmaatschappij.

Beoordeling door de EDPB

---

[105] De FR TA heeft verduidelijkt dat dit ter illustratie is en dat niet in de EER gevestigde cloudaanbieders ook in aanmerking kunnen worden genomen. Daarnaast zouden ook andere opslagoplossingen (bv. zonder gebruikmaking van de cloud) kunnen worden overwogen.

[106] De FR TA heeft verduidelijkt dat dit ter illustratie is en dat er een oplossing is waarbij voorafgaand aan elke vlucht biometrische gegevens worden doorgegeven.

84. De door het Comité reeds gemaakte opmerkingen met betrekking tot scenario 3.1[107] zijn ook op dit scenario van toepassing.

85. Wat betreft het beginsel en de vereisten met betrekking tot de beveiliging (artikel 5, lid 1, punt f), en artikel 32 AVG) vindt de verwerking in scenario 3.2 plaats in de cloud, en meerdere entiteiten zouden toegang tot deze gegevens kunnen hebben, waaronder mogelijk niet-EER-aanbieders, zelfs wanneer de gegevens in de EER worden bewaard[108]. Een dergelijke architectuur brengt potentiële risico's met zich mee met betrekking tot doorgiften van persoonsgegevens aan derde landen. Daarnaast worden de gegevens van de passagiers weliswaar versleuteld, maar tijdens het gebruik (d.w.z. wanneer de matching wordt uitgevoerd) gedecodeerd, terwijl de sleutels worden beheerd door de luchtvaartmaatschappij of haar cloudverwerker. Een dergelijke opslag kan leiden tot een verdere toename van de blootstelling aan beveiligingsrisico's.

86. Wat betreft de verenigbaarheid met artikel 5, lid 1, punt f), en artikel 32 AVG zijn de in scenario 3.2 beoogde maatregelen[109], rekening houdend met de stand van de techniek, derhalve ontoereikend om een op het risico afgestemd beveiligingsniveau te waarborgen. Op grond van het bovenstaande zou de verwerking in scenario 3.2 niet voldoen aan artikel 5, lid 1, punt f), en artikel 32 AVG indien een verwerkingsverantwoordelijke zich tot deze maatregelen zou beperken.

87. Daarnaast kunnen de gegevens, overeenkomstig scenario 3.2[110], worden opgeslagen gedurende een aanzienlijke periode (die zo lang kan zijn als de betrokkene een account heeft bij de luchtvaartmaatschappij). Met een dergelijke opslagduur worden de gegevens blootgesteld aan een hoger risico van een inbreuk op de vertrouwelijkheid en integriteit ervan, en deze opslagduur lijkt verder te gaan dan strikt noodzakelijk en evenredig is met het oog op de verwerking. Het Comité merkt op dat de gegevensopslagperiode op zich geen doorslaggevende factor is voor de algemene verenigbaarheid van de betrokken architectuur met de AVG, aangezien deze termijn door de verwerkingsverantwoordelijken kan worden gewijzigd. Op grond van de informatie die het Comité ter beschikking staat en die in de beschrijving van scenario 3.2 is opgenomen, is er echter geen voldoende rechtvaardiging voor deze lange bewaartermijn en zijn er geen duidelijke maatregelen om de risico's voor individuen te beperken. Op basis hiervan zou de voorgestelde opslagperiode niet beperkt blijven tot wat noodzakelijk is, overeenkomstig het beginsel van opslagbeperking van artikel 5, lid 1, punt e), AVG.

88. In elk geval kunnen de voorgestelde maatregelen in scenario 3.2 niet voldoen aan de vereisten inzake gegevensbescherming door ontwerp en door standaardinstellingen van artikel 25 AVG. In scenario 3.2 worden de geregistreerde biometrische templates van de passagiers opgeslagen in de cloud, onder de controle van de luchtvaartmaatschappij of haar cloudaanbieder (gegevensverwerker). Zoals hierboven is beschreven, zouden meerdere entiteiten toegang tot deze gegevens kunnen hebben. Bovendien worden de biometrische gegevens van de passagiers gebruikt voor de identificatie van de passagiers (één-op-n-vergelijking), waarbij n maximaal het totale aantal gebruikers/klanten van de luchtvaartmaatschappij is. Een dergelijke methode houdt in dat in een groep individuen in de centrale

[107] Punten 68-77.
[108] Gecoördineerde handhavingsactie betreffende het gebruik van clouddiensten door de publieke sector 2022 van de EDPB van 17 januari 2023, blz. 19.
[109] Zie de punten 79-83.
[110] Zie punt 83.

databank een persoon moet worden gevonden door elk vastgelegd gezicht te verwerken om te controleren of het overeenkomt met een persoon die bekend is bij het systeem. In tegenstelling tot scenario 3.1 zou in scenario 3.2 de vergelijking op een veel grotere schaal kunnen worden uitgevoerd, aangezien het criterium hier het totale aantal klanten van de luchtvaartmaatschappij is, terwijl in scenario 3.1 slechts het aantal binnen een tijdsbestek van enkele dagen verwachte passagiers is opgenomen.

89. Bovendien kan de in scenario 3.2 beoogde verwerking wat betreft de verenigbaarheid met artikel 25 AVG, en met name om te voldoen aan het vereiste van minimale gegevensverwerking, niet beantwoorden aan het noodzaakbeginsel. Het Comité is van mening dat een soortgelijk resultaat om de passagiersstroom op luchthavens te stroomlijnen kan worden bereikt met andere maatregelen die minder indringend zijn, bijvoorbeeld zonder dat er biometrische gegevens worden gebruikt, hoewel de gebruikerservaring in dat geval anders zou zijn, aangezien het tonen van de ID-kaart en de instapkaart dan meer tijd in beslag zou kunnen nemen. Bovendien kan de verwerkingsverantwoordelijke met andere oplossingen, met name die welke zijn gebaseerd op de opslag van de biometrische gegevens in een lokale portemonnee op het apparaat van het individu of oplossingen waarbij de gegevens moeten worden versleuteld met een specifieke sleutel die wordt opgeslagen op het apparaat van het individu, de doelstellingen bereiken op een manier waarbij minder inbreuk op de privacy wordt gemaakt.

90. Wat het evenredigheidsbeginsel betreft, zou de in scenario 3.2 beoogde verwerking risico's voor de rechten van de betrokkenen met zich meebrengen die door de beoogde waarborgen niet zouden worden beperkt. De negatieve gevolgen voor de grondrechten en de fundamentele vrijheden van de betrokkenen die zouden voortvloeien uit een inbreuk in verband met persoonsgegevens in een gecentraliseerde databank met in de cloud opgeslagen biometrische gegevens van een groot aantal personen, lijken zwaarder te wegen dan het verwachte voordeel dat uit de verwerking voortvloeit, aangezien een dergelijk voordeel relatief gering is, d.w.z. een lichte toename van het gemak en de snelheid van de controles. Dit voordeel kan dan ook geen rechtvaardiging vormen voor de grote indringendheid van die maatregelen met betrekking tot de grondrechten en de fundamentele vrijheden van natuurlijke personen, en de in scenario 3.2 beoogde verwerking kan niet als evenredig worden beschouwd.

91. In het licht van deze overwegingen concludeert het Comité, in antwoord op vraag 2.3.1, dat, indien de verwerking plaatsvindt met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen, de in scenario 3.2 beoogde verwerking:

- **niet verenigbaar kan zijn met artikel 25 AVG**;
- **niet zou voldoen aan artikel 5, lid 1, punt f), en artikel 32 AVG** indien een verwerkingsverantwoordelijke zich zou beperken tot de in scenario 3.2 beschreven maatregelen;
- **niet zou voldoen aan artikel 5, lid 1, punt e), AVG**, aangezien er op basis van de informatie die het Comité ter beschikking staat geen voldoende rechtvaardiging is voor de in scenario 3.2 beoogde bewaartermijn. Om te voldoen aan het beginsel van opslagbeperking van artikel 5, lid 1, punt e), AVG, zou de verwerkingsverantwoordelijke moeten aantonen dat persoonsgegevens niet langer worden opgeslagen dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

4 CONCLUSIES

92. Wat vraag 1.1 betreft, concludeert het Comité, op basis van het verzoek om een advies van de FR TA, met betrekking tot de vereisten van artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG, en op basis van de bovenstaande analyse, dat:

93. het gebruik van gezichtsherkenningstechnologie voor biometrische authenticatie met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen (beveiligingscontroleposten, het inchecken van bagage, het instappen en de toegang tot de passagierslounge), in beginsel verenigbaar kan worden geacht met de beginselen van integriteit en vertrouwelijkheid overeenkomstig artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG, in het geval van een opslagarchitectuur waarbij de geregistreerde biometrische template van elke passagier op lokaal niveau wordt opgeslagen op zijn persoonlijke apparaat en onder zijn uitsluitende controle, mits in passende waarborgen wordt voorzien zoals beschreven vanaf punt 46.

94. Wat vraag 2.1.1 betreft, concludeert het Comité, op basis van het verzoek om een advies van de FR TA, met betrekking tot de vereisten van artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG, en op basis van de bovenstaande analyse, dat:

95. het gebruik van gezichtsherkenningstechnologie voor biometrische authenticatie met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen (beveiligingscontroleposten, het inchecken van bagage, het instappen en de toegang tot de passagierslounge), in beginsel verenigbaar kan worden geacht met het beginsel van opslagbeperking overeenkomstig artikel 5, lid 1, punt e), en de beginselen van integriteit en vertrouwelijkheid overeenkomstig artikel 5, lid 1, punt f), en de artikelen 25 en 32 AVG, in het geval van een gecentraliseerde opslagarchitectuur waarbij de geregistreerde biometrische template van elke passagier wordt opgeslagen in een centrale databank binnen de luchthaven, onder de controle van de luchthavenexploitant, in versleutelde vorm, met een sleutel/geheim die/dat uitsluitend in handen is van het individu, mits in passende waarborgen wordt voorzien zoals beschreven vanaf punt 60.

96. Wat vraag 2.2.1 betreft, concludeert het Comité, op basis van het verzoek om een advies van de FR TA, met betrekking tot de vereisten van artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG, en op basis van de bovenstaande analyse, dat:

97. het gebruik van gezichtsherkenningstechnologie voor biometrische identificatie met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen (beveiligingscontroleposten, het inchecken van bagage, het instappen en de toegang tot de passagierslounge) in het geval van een gecentraliseerde opslagarchitectuur, wanneer de geregistreerde biometrische templates van de passagiers niet worden versleuteld met een sleutel/geheim die/dat uitsluitend in handen is van elke passagier, waarbij deze templates worden opgeslagen in een databank binnen de luchthaven (onder de controle van de luchthavenexploitant), niet verenigbaar kan zijn met artikel 25 AVG. Bovendien zou een dergelijke verwerking niet voldoen aan het beginsel van integriteit en vertrouwelijkheid overeenkomstig artikel 5, lid 1, punt f), en artikel 32 AVG indien een verwerkingsverantwoordelijke zich zou beperken tot de in scenario 3.1 beschreven maatregelen.

98. Wat vraag 2.3.1 betreft, concludeert het Comité, op basis van het verzoek om een advies van de FR TA, met betrekking tot de vereisten van artikel 5, lid 1, punten e) en f), en de artikelen 25 en 32 AVG, en op basis van de bovenstaande analyse, dat:

99. het gebruik van gezichtsherkenningstechnologie voor biometrische identificatie met het specifieke doel om de passagiersstroom op luchthavens te stroomlijnen (beveiligingscontroleposten, het

inchecken van bagage, het instappen en de toegang tot de passagierslounge) in het geval van een gecentraliseerde opslagarchitectuur, wanneer de geregistreerde biometrische templates van de passagiers niet worden versleuteld met een sleutel/geheim die/dat uitsluitend in handen is van elke passagier, waarbij deze templates worden opgeslagen in de cloud (onder de controle van de luchtvaartmaatschappij), niet verenigbaar kan zijn met artikel 25 AVG. Bovendien zou een dergelijke verwerking niet voldoen aan de beginselen van integriteit en vertrouwelijkheid overeenkomstig artikel 5, lid 1, punt f), en artikel 32 AVG indien een verwerkingsverantwoordelijke zich zou beperken tot de in scenario 3.2 beschreven maatregelen. Ten slotte zou de verwerking, op basis van de beschrijving van scenario 3.2 en de informatie die het Comité ter beschikking staat, niet voldoen aan het beginsel van opslagbeperking overeenkomstig artikel 5, lid 1, punt e), AVG.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Anu Talus)