Stellungnahme des EDSA nach Artikel 64 DSGVO

Stellungnahme Nr. 11/2024 zum Einsatz von Gesichtserkennung zur Straffung der Fluggastströme (Vereinbarkeit mit Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und Artikel 32 DSGVO)

Version 1.1

Angenommen am 23. Mai 2024

Version 1.1	28. Mai 2024	Grammatikalische Korrektur in der Zusammenfassung (Seiten 3 und 4) sowie Rn. 77 und 90 der Stellungnahme
Version 1.0	23. Mai 2024	Annahme der Stellungnahme

Zusammenfassung

Die französische Aufsichtsbehörde hat den Europäischen Datenschutzausschuss um eine Stellungnahme zum Einsatz von Gesichtserkennungstechnologie durch Flughafenbetreiber und Fluggesellschaften zur biometrischen Authentifizierung oder Identifizierung von Fluggästen zum Zweck der Straffung der Fluggastströme ersucht.

Vorab weist der Ausschuss erneut darauf hin, dass die Nutzung biometrischer Daten und insbesondere von Gesichtserkennungstechnologie erhöhte Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringt. Dies betrifft die Verarbeitung biometrischer Daten, die gemäß Artikel 9 DSGVO besonderen Schutz genießen. Selbst wenn derartige Technologien als besonders wirksam angesehen würden, sollten die Verantwortlichen vor deren Einsatz die Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen beurteilen und prüfen, ob sie ihren legitimen Zweck der Verarbeitung mit weniger einschneidenden Mitteln erreichen können.

Gemäß dem Antrag ist der Anwendungsbereich der vorliegenden Stellungnahme auf die Frage beschränkt, ob die Verarbeitung für den **spezifischen Zweck der Straffung der Fluggastströme** an vier bestimmten Kontrollpunkten, nämlich bei den Sicherheitskontrollen, bei der Gepäckaufgabe, beim Boarding und beim Zugang zur Fluggastlounge, mit **Artikel 5 Absatz 1 Buchstaben e und f sowie mit den Artikeln 25 und 32 DSGVO** vereinbar ist. Die vorliegende Stellungnahme enthält keine erschöpfende und vollständige Analyse der Einhaltung der DSGVO durch den bzw. die jeweiligen Verantwortlichen sowie gegebenenfalls deren Auftragsverarbeiter. Somit greift die vorliegende Stellungnahme einer rechtlichen und technischen Einzelfallanalyse, die auf der spezifischen geplanten Verarbeitung durch einen Verantwortlichen und den spezifischen Umständen beruht, nicht vor. Darüber hinaus fällt die Analyse der anwendbaren Rechtsgrundlage nicht in den Anwendungsbereich der dem Ausschuss in dem Antrag vorgelegten Fragen, sodass die Gültigkeit der Zustimmung zu einer solchen Verarbeitung gemäß den Artikeln 6, 7 und 9 DSGVO in der vorliegenden Stellungnahme nicht geprüft wird. Des Weiteren lässt die vorliegende Stellungnahme die im Recht der Mitgliedstaaten festgelegten Beschränkungen im Hinblick auf die Verwendung biometrischer Daten unberührt.

In der vorliegenden Stellungnahme bewertet der Ausschuss im Zusammenhang mit **vier spezifischen Szenarien** die Vereinbarkeit der Verarbeitung mit den genannten Bestimmungen der DSGVO.

Das **erste Szenario** betrifft die Speicherung eines registrierten biometrischen Templates im Zugriff der Einzelperson, z. B. auf ihrem eigenen Gerät, unter ihrer alleinigen Kontrolle, um den Fluggast an den genannten Kontrollpunkten auf dem Flughafen zu authentifizieren (1:1-Abgleich).

Der Ausschuss kommt zu dem Schluss, dass davon ausgegangen werden kann, dass die gewählten Maßnahmen dem Grundsatz der Notwendigkeit entsprechen, wenn der Verantwortliche nachweisen kann, dass es keine weniger einschneidenden alternativen Lösungen gibt, mit denen dasselbe Ziel ebenso wirksam erreicht werden könnte. Darüber hinaus kann die Intensität des Eingriffs bei der Verarbeitung durch die aktive Beteiligung der Fluggäste kompensiert werden, da ihr biometrisches Template in ihrem ausschließlichen Zugriff, z. B. auf ihrem eigenen Gerät, unter ihrer alleinigen Kontrolle gespeichert wird und ihre Daten kurz nach Beendigung des Abgleichs gelöscht werden. Auf dieser Grundlage kommt der Ausschuss zu dem Schluss, dass die im ersten Szenario vorgesehene Verarbeitung vorbehaltlich der Umsetzung geeigneter Garantien **grundsätzlich als mit Artikel 5 Absatz 1 Buchstabe f, Artikel 25 und Artikel 32 DSGVO vereinbar angesehen werden könnte**.

Der Ausschuss hat Garantien ermittelt, die mindestens umgesetzt werden sollten, um eine Lösung, die dem ersten Szenario ähnelt, zu erreichen.

Das **zweite Szenario** betrifft die zentrale Speicherung eines registrierten biometrischen Templates in verschlüsselter Form mit einem Schlüssel/Passwort, der sich ausschließlich im Zugriff des Fluggastes befindet, in den Einrichtungen des Flughafens. Dadurch wird die Authentifizierung der Fluggäste (1:1-Abgleich) ermöglicht, während sie die genannten Flughafenkontrollpunkte durchlaufen. Die Registrierung ist für einen bestimmten Zeitraum gültig, beispielsweise bis zu einem Jahr nach Antritt des letzten Fluges oder bis zum Ablaufdatum des Reisepasses.

Der Ausschuss kommt zu dem Schluss, dass davon ausgegangen werden kann, dass die Verarbeitung dem Grundsatz der Notwendigkeit entspricht, wenn der Verantwortliche nachweisen kann, dass es keine weniger einschneidenden alternativen Lösungen gibt, mit denen dasselbe Ziel ebenso wirksam erreicht werden könnte. Darüber hinaus kann die Intensität des Eingriffs bei der Verarbeitung durch die aktive Beteiligung des Fluggastes kompensiert werden, da sich seine verschlüsselten biometrischen Daten unter seiner alleinigen Kontrolle befinden. Unter der Annahme, dass der Verantwortliche geeignete Garantien umsetzt, könnten die Sicherheitsrisiken in diesem Szenario durch die Nutzung einer zentralen Datenbank abgemildert werden, und es kann davon ausgegangen werden, dass die negativen Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen in einem angemessenen Verhältnis zum erwarteten Nutzen stehen. Was den Grundsatz der Speicherbegrenzung betrifft, so wurden dem Ausschuss keine Informationen zur Begründung der langen Speicherfrist übermittelt. Um in diesem Szenario die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstabe e DSGVO zu erreichen, sollten die Verantwortlichen begründen können, warum in bestimmten Fällen die geplante Speicherfrist für den Zweck erforderlich ist. Der Ausschuss empfiehlt, dass die Verantwortlichen eine möglichst kurze Speicherfrist vorsehen und gleichzeitig den Fluggästen die Möglichkeit bieten, die von ihnen bevorzugte Speicherfrist festzulegen. Auf dieser Grundlage kommt der Ausschuss zu dem Schluss, dass die in Szenario 2 vorgesehene Verarbeitung vorbehaltlich der Anwendung geeigneter Garantien **grundsätzlich als mit Artikel 5 Absatz 1 Buchstabe e, Artikel 5 Absatz 1 Buchstabe f, Artikel 25 und Artikel 32 DSGVO vereinbar angesehen werden könnte**.

Der Ausschuss hat Garantien ermittelt, die mindestens umgesetzt werden sollten, um eine Lösung, die dem zweiten Szenario ähnelt, zu erreichen.

Das **dritte Szenario** betrifft die zentrale Speicherung eines registrierten biometrischen Templates in verschlüsselter Form unter der Kontrolle des Flughafenbetreibers in den Einrichtungen des Flughafens. Dadurch wird die Identifizierung der Fluggäste (1:N-Abgleich) ermöglicht, während sie die genannten Kontrollpunkte auf dem Flughafen durchlaufen. In diesem Szenario beträgt die Speicherfrist in der Regel 48 Stunden, und die Daten werden gelöscht, sobald das Flugzeug gestartet ist.

Da die Speicherung der Identitäts- und biometrischen Daten in einer zentralen Datenbank erfolgt, könnten im Fall der Beeinträchtigung der Vertraulichkeit der Datenbank in der Folge der Zugriff auf den gesamten Datenbestand und eine unbefugte oder unzulässige Identifizierung von Fluggästen in anderen Umgebungen ermöglicht werden. Die zentrale Speicherarchitektur unter der Kontrolle des Flughafenbetreibers hat außerdem zur Folge, dass die Fluggäste in größerem Umfang die Kontrolle über ihre Daten verlieren. Im Hinblick auf die Straffung des Fluggaststroms auf Flughäfen ist der Ausschuss der Auffassung, dass sich ein ähnliches Ergebnis auf weniger einschneidende Weise erreichen ließe und dass die negativen Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen, die sich aus einer Verletzung des Datenschutzes in einer zentralen Datenbank biometrischer Daten ergeben würden, den erwarteten Nutzen infolge der Verarbeitung zu

überwiegen scheinen. Daher kann die Verarbeitung nicht den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit entsprechen. Auf dieser Grundlage kommt der Ausschuss zu dem Schluss, dass die im dritten Szenario vorgesehene Verarbeitung **nicht mit Artikel 25 DSGVO vereinbar sein kann**. Außerdem wäre es **nicht mit Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO vereinbar**, wenn sich ein Verantwortlicher auf die in diesem Szenario beschriebenen Maßnahmen beschränken würde.

Das **vierte Szenario** betrifft die zentrale Speicherung eines registrierten biometrischen Templates in verschlüsselter Form in der Cloud unter der Kontrolle der Fluggesellschaft oder ihres Cloud-Diensteanbieters. Dadurch wird die Identifizierung der Fluggäste (1:N-Abgleich) ermöglicht während sie die genannten Kontrollpunkte auf dem Flughafen durchlaufen. Die Speicherfrist in diesem Szenario kann so lange andauern, wie der Kunde ein Konto bei der Fluggesellschaft hat.

Da die Speicherung der Identitätsdaten und der biometrischen Daten in einer zentralen Cloud-Datenbank erfolgt, könnten mehrere Einrichtungen Zugang zu diesen Daten haben, darunter möglicherweise auch Anbieter außerhalb des EWR. Die Daten des Fluggastes werden bei Verwendung entschlüsselt, und die Schlüssel stehen unter der Kontrolle der Fluggesellschaft oder ihrer Auftragsverarbeiter, wodurch sich die Angriffsfläche für eine Sicherheitsgefährdung vergrößern könnte. Eine zentrale Speicherarchitektur dieser Art hat außerdem zur Folge, dass die Fluggäste in größerem Umfang die Kontrolle über ihre Daten verlieren. Zudem könnten die Daten für einen erheblichen Zeitraum gespeichert werden, wodurch die Daten einem höheren Risiko einer Sicherheitsverletzung ausgesetzt sind und das für die Zwecke der Verarbeitung unbedingt erforderliche und verhältnismäßige Maß offenbar überschritten wird, es sei denn, es werden erkennbar weitere Maßnahmen ergriffen, um die Risiken für Einzelpersonen zu mindern.

Der Ausschuss ist der Auffassung, dass sich im Hinblick auf die Straffung des Fluggaststroms auf Flughäfen ein ähnliches Ergebnis auf weniger einschneidende Weise erreichen ließe und dass die negativen Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen, die sich aus einer Verletzung des Datenschutzes in einer zentralen Datenbank biometrischer Daten ergeben könnten, den erwarteten Nutzen infolge der Verarbeitung zu überwiegen scheinen. Daher kann die Verarbeitung nicht den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit entsprechen. Auf dieser Grundlage kommt der Ausschuss zu dem Schluss, dass die im vierten Szenario vorgesehene Verarbeitung **nicht mit Artikel 25 DSGVO vereinbar sein kann**. Außerdem wäre es ausgehend von den dem Ausschuss zur Verfügung stehenden Informationen **nicht mit Artikel 5 Absatz 1 Buchstabe e DSGVO** und **Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO vereinbar**, wenn sich ein Verantwortlicher auf die in diesem Szenario beschriebenen Maßnahmen beschränken würde.

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 63 und Artikel 64 Absatz 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (im Folgenden „**DSGVO**“),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung[1],

gestützt auf Artikel 10 und Artikel 22 der Geschäftsordnung des Europäischen Datenschutzausschusses (im Folgenden „**Ausschuss**“ oder „**EDSA**“),

in Erwägung nachstehender Gründe:

(1) Die Hauptaufgabe des Ausschusses besteht darin, die einheitliche Anwendung der DSGVO im gesamten Europäischen Wirtschaftsraum (im Folgenden „**EWR**“) sicherzustellen. Gemäß Artikel 64 Absatz 2 DSGVO kann jede Aufsichtsbehörde, der Vorsitz des Ausschusses oder die Kommission beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem EWR-Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten.

(2) Die Stellungnahme des Ausschusses wird gemäß Artikel 64 Absatz 3 DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung des EDSA innerhalb von acht Wochen, nachdem der Vorsitz und die zuständige Aufsichtsbehörde entschieden haben, dass das Dossier vollständig ist, angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um weitere sechs Wochen verlängert werden.

hat folgende Stellungnahme angenommen:

1 EINLEITUNG

1.1 Sachverhalt

1. Am 16. Februar 2024 ersuchte die französische Aufsichtsbehörde den Ausschuss um eine Stellungnahme zur Vereinbarkeit des Einsatzes von Gesichtserkennungstechnologie durch Flughafenbetreiber und Fluggesellschaften zur biometrischen Authentifizierung oder Identifizierung von Fluggästen[2] zum Zweck der Straffung der Fluggastströme bei den Flughafen-Sicherheitskontrollen[3], bei der Gepäckaufgabe, beim Boarding und beim Zugang zur Fluggastlounge auf Flughäfen (ausgenommen Grenzkontrollen und Kontrollen durch Duty-free-Shops) mit Artikel 5

[1] Soweit in dieser Stellungnahme auf „**Mitgliedstaaten**“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen. Soweit in dieser Stellungnahme auf die „Union“ oder „EU“ Bezug genommen wird, ist dies als Bezugnahme auf den „EWR“ zu verstehen.

[2] Im Zusammenhang mit dieser Stellungnahme bezeichnet der Ausdruck „**Fluggast**“ eine betroffene Person, deren personenbezogene Daten für den in der vorliegenden Stellungnahme beschriebenen spezifischen Zweck verarbeitet werden. Im Folgenden werden die Begriffe „Fluggast“ und „Einzelperson“ austauschbar verwendet.

[3] Für die Zwecke dieser Stellungnahme beziehen sich „**Flughafen-Sicherheitskontrollen**“ auf die Sicherheitskontrollen, die unter der Verantwortung des Flughafenbetreibers durchgeführt werden und denen sich die Fluggäste unterziehen müssen, um von der Abflughalle aus den Abflugbereich oder die Flugsteige zu betreten.

Absatz 1 Buchstaben e und f sowie mit den Artikeln 25 und 32 DSGVO (im Folgenden „**Antrag**“). Die französische Aufsichtsbehörde hat ihrem Antrag eine Beschreibung der typischen Anwendungsfälle beigefügt (Anhang I).

2. In ihrem Antrag stellt die französische Aufsichtsbehörde fest, dass die Modelle, die derzeit an mehreren EU-Flughäfen getestet werden, von Mitgliedstaat zu Mitgliedstaat unterschiedlich sind, wodurch möglicherweise die Gefahr besteht, dass die Auslegungen der Aufsichtsbehörden voneinander abweichen und sich unterschiedliche Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen in der EU ergeben.[4]

3. Der Ausschuss ist der Auffassung, dass zur Beantwortung des Antrags folgende Fragen zu beantworten sind:

4. **Frage 1**:

1.1. Kann der Einsatz von Gesichtserkennungstechnologie zur biometriegestützten Authentifizierung **zu dem spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen** (Sicherheitskontrollen, Gepäckaufgabe, Boarding und Zugang zur Fluggastlounge) im Falle einer Speicherarchitektur, bei der das biometrische Template jedes Fluggastes **ausschließlich im Zugriff der Einzelperson**, z. B. lokal auf ihrem eigenen Gerät, unter ihrer alleinigen Kontrolle gespeichert wird, mit **Artikel 5 Absatz 1 Buchstabe f, Artikel 25 und Artikel 32 DSGVO** vereinbar sein?

1.2. Würde eine derartige Verarbeitung als mit den genannten Bestimmungen vereinbar angesehen, welche angemessenen Mindestgarantien wären dann im Hinblick auf die Artikel 25 und 32 DSGVO erforderlich?

Frage 2:

2.1. Kann der Einsatz von Gesichtserkennungstechnologie zur biometriegestützten Authentifizierung oder Identifizierung **zu dem spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen** (Sicherheitskontrollen, Gepäckaufgabe, Boarding und Zugang zur Fluggastlounge) mit **Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und 32 DSGVO** vereinbar sein, wenn eine **zentrale** Speicherarchitektur verwendet wird, bei der das biometrische Template jedes Fluggastes in einer zentralen Datenbank gespeichert wird:

2.1.1. In einer zentralen Datenbank in den Einrichtungen des Flughafens unter der Kontrolle des Flughafenbetreibers in verschlüsselter Form mit einem Schlüssel/Passwort, der bzw. das ausschließlich im Zugriff der Einzelperson (z. B. im Mobiltelefon der Person) zur Authentifizierung aufbewahrt wird?

2.1.2. Würde eine derartige Verarbeitung als vereinbar angesehen, welche angemessenen Mindestgarantien wären dann im Hinblick auf die Artikel 25 und 32 DSGVO erforderlich?

[4] Antrag, S. 1.

2.2.1. In einer zentralen Datenbank in den Einrichtungen des Flughafens unter der Kontrolle des Flughafenbetreibers, in verschlüsselter Form mit Schlüsseln, die vom Flughafenbetreiber zur Identifizierung aufbewahrt werden?

2.2.2. Würde eine derartige Verarbeitung als vereinbar angesehen, welche angemessenen Mindestgarantien wären dann im Hinblick auf die Artikel 25 und 32 DSGVO erforderlich?

2.3.1. In der Cloud unter der Kontrolle der Fluggesellschaft oder ihres Dienstleisters (Auftragsverarbeiters) in verschlüsselter Form mit Schlüsseln, die von der Fluggesellschaft oder ihrem Dienstleister zur Identifizierung aufbewahrt werden?

2.3.2. Würde eine derartige Verarbeitung als vereinbar angesehen, welche angemessenen Mindestgarantien wären dann im Hinblick auf die Artikel 25 und 32 DSGVO erforderlich?

5. Nachdem die französische Aufsichtsbehörde das Dossier am 16. Februar 2024 für vollständig erachtete und der Vorsitz des Ausschusses am 23. Februar 2024, wurde das Dossier am 23. Februar 2024 vom Sekretariat in Umlauf gebracht. Der Vorsitz des Ausschusses hat im Einklang mit Artikel 64 Absatz 3 DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung des EDSA beschlossen, die Standardfrist von acht Wochen unter Berücksichtigung der Komplexität der Angelegenheit um weitere sechs Wochen zu verlängern.

1.2 Zulässigkeit des Antrags auf eine Stellungnahme nach Artikel 64 Absatz 2 DSGVO

6. Gemäß Artikel 64 Absatz 2 der DSGVO kann insbesondere jede Aufsichtsbehörde beantragen, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten.

7. Der Ausschuss ist der Auffassung, dass sich der von der französischen Aufsichtsbehörde eingereichte Antrag zur Vereinbarkeit des Einsatzes von Gesichtserkennungstechnologie zur biometrischen Authentifizierung oder Identifizierung zu dem spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen auf Fragen „mit Auswirkungen in mehr als einem Mitgliedstaat“ bezieht, da, wie im Antrag[5] erläutert, derzeit auf den Flughäfen der Mitgliedstaaten mehrere Projekte umgesetzt werden und davon ausgegangen wird, dass Anwendungen dieser Art in den kommenden Jahren zunehmen werden. Die Modelle, die derzeit von verschiedenen Flughäfen und Fluggesellschaften getestet werden, unterscheiden sich von Mitgliedstaat zu Mitgliedstaat erheblich, sodass möglicherweise aus datenschutzrechtlicher Sicht die Gefahr besteht, dass in mehr als einem Mitgliedstaat unterschiedliche Auswirkungen auftreten.

8. Ferner ist der Ausschuss der Auffassung, dass der Antrag, der von der französischen Aufsichtsbehörde eingereicht wurde, erhebliche Auswirkungen auf die Anwendung der in Artikel 5 Absatz 1 Buchstaben e und f DSGVO festgelegten Grundsätze und die Anforderungen an Verantwortliche nach Artikel 25 DSGVO sowie die Anforderungen an Verantwortliche und Auftragsverarbeiter gemäß Artikel 32 DSGVO hat. Daher betrifft dieser Antrag eine „Angelegenheit allgemeiner Geltung“ im Sinne von Artikel 64 Absatz 2 DSGVO, da er sich auf die einheitliche Auslegung der Grundsätze der Speicherbegrenzung (Artikel 5 Absatz 1 Buchstabe e DSGVO) und der Integrität und Vertraulichkeit

[5] Antrag, S. 3.

(Artikel 5 Absatz 1 Buchstabe f DSGVO) sowie die Begriffe Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen (Artikel 25 DSGVO) und Datensicherheit (Artikel 32 DSGVO) bezieht, um unter anderem für die einheitliche Anwendung dieser Bestimmungen im EWR zu sorgen.

9. Etwaige unterschiedliche Standpunkte der Mitgliedstaaten zur Auslegung von Artikel 5 Absatz 1 Buchstaben e und f sowie der Artikel 25 und 32 DSGVO würden das Risiko erhöhen, dass Flughafenbetreiber und Fluggesellschaften Gesichtserkennungsprojekte nicht auf einheitliche Weise entwickeln. Da die französische Aufsichtsbehörde die eindeutige Notwendigkeit einer einheitlichen Auslegung dieser Bestimmungen im Hinblick auf die Gesichtserkennungstechnologie zur biometrischen Authentifizierung oder Identifizierung zum Zweck der Straffung des Fluggaststroms auf Flughäfen[6] nachgewiesen hat, ist der Ausschuss der Auffassung, dass der Antrag im Einklang mit Artikel 10 Absatz 3 der Geschäftsordnung des EDSA begründet ist.

10. Gemäß Artikel 64 Absatz 3 DSGVO gibt der EDSA keine Stellungnahme ab, wenn er bereits eine Stellungnahme zu derselben Angelegenheit abgegeben hat.[7] Der EDSA hat die Fragen, die sich aus dem Antrag ergeben, noch nicht beantwortet. Die EDSA-Leitlinien 3/2019 zu Videogeräten[8] enthalten zwar bereits einige nützliche Elemente zu den Sicherheitsvorkehrungen, die bei der Verarbeitung biometrischer Daten angewandt werden sollten, jedoch wird darin nicht auf alle Aspekte im Zusammenhang mit den im Antrag vorgelegten Fragen eingegangen. Darüber hinaus enthalten die verfügbaren Leitlinien des EDSA, einschließlich der EDSA-Leitlinien 3/2019 zu Videogeräten, keine spezifischen Leitlinien zu möglichen Elementen, die im Zusammenhang mit der zentralen oder dezentralen Speicherung biometrischer Daten zur Identifizierung oder Authentifizierung von Fluggästen zum Zweck der Straffung des Fluggaststroms auf Flughäfen zu überprüfen sind, und zur Vereinbarkeit einer derartigen Verarbeitung mit Artikel 5 Absatz 1 Buchstaben e und f sowie den Artikeln 25 und 32 DSGVO.

11. Aus diesen Gründen ist der Ausschuss der Auffassung, dass der Antrag zulässig ist und die darin vorgelegten Fragen in einer gemäß Artikel 64 Absatz 2 DSGVO angenommenen Stellungnahme analysiert werden sollten.

2 ANWENDUNGSBEREICH UND HINTERGRUND DER STELLUNGNAHME

2.1 Anwendungsbereich der Stellungnahme

12. Gemäß dem Antrag betrifft die vorliegende Stellungnahme ausschließlich die Frage, ob der Einsatz von Gesichtserkennungstechnologie zur biometriegestützten Authentifizierung oder Identifizierung von Fluggästen durch Flughafenbetreiber und Fluggesellschaften **zu dem spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen**, nämlich bei den Sicherheitskontrollen, bei der Gepäckaufgabe, beim Boarding und beim Zugang zur Fluggastlounge, mit Artikel 5 Absatz 1 Buchstaben e und f und den Artikeln 25 und 32 DSGVO vereinbar ist.

13. In Bezug auf den **Anwendungsbereich dieser Stellungnahme** stellt der Ausschuss Folgendes klar:

[6] Antrag, S. 1.
[7] Artikel 64 Absatz 3 DSGVO und Artikel 10 Absatz 4 der Geschäftsordnung des EDSA.
[8] EDSA-Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, angenommen am 29. Januar 2020 (im Folgenden **EDSA-Leitlinien 3/2019 zu Videogeräten**).

1) Die Verarbeitung personenbezogener Daten im Rahmen von Grenzkontrollen und Kontrollen durch Duty-free-Shops fällt nicht in den Anwendungsbereich dieser Stellungnahme, da sie von anderen Verantwortlichen als Flughafenbetreibern und Fluggesellschaften durchgeführt wird.

2) Auch wenn die Gesichtserkennungstechnologie auf den in Abschnitt 3.2 beschriebenen Szenarien beruht, fällt ihr Einsatz für andere Zwecke (z. B. Strafverfolgung) oder durch andere Einrichtungen, selbst wenn sie ähnliche Zwecke verfolgen, nicht unter den Anwendungsbereich dieser Stellungnahme.

3) In der vorliegenden Stellungnahme wird ausschließlich die Verarbeitung personenbezogener Daten von Fluggästen untersucht, und es werden keine anderen Kategorien betroffener Personen, wie das Personal der Flughafenbetreiber oder der Fluggesellschaften, behandelt.

4) Der Antrag der französischen Aufsichtsbehörde wird in der vorliegenden Stellungnahme im Hinblick auf die Vereinbarkeit der Speicherarchitekturen der biometrischen Templates der Fluggäste mit Artikel 5 Absatz 1 Buchstaben e und f sowie den Artikeln 25 und 32 DSGVO geprüft. In dieser Hinsicht enthält die vorliegende Stellungnahme keine umfassende und vollständige Analyse der Einhaltung der DSGVO durch den bzw. die jeweiligen Verantwortlichen sowie gegebenenfalls deren Auftragsverarbeiter. Dies ist insbesondere wichtig, da diese Technologien mit erhöhten Risiken im Zusammenhang mit der Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO einhergehen. Daher greift diese Stellungnahme im Hinblick auf den Einsatz von Gesichtserkennungstechnologien, auch in dem spezifischen Bereich, auf den sich der Antrag bezieht, weder einer Bewertung anderer Bestimmungen der DSGVO noch der rechtlichen und technischen Einzelfallanalyse auf der Grundlage der spezifischen geplanten Verarbeitung durch einen Verantwortlichen und der spezifischen Umstände vor.

5) Die vorliegende Stellungnahme umfasst nicht die Verarbeitung personenbezogener Daten von Kindern und lässt spezifische Anforderungen, die in dieser Hinsicht gelten, unberührt.

6) Rechtliche Anforderungen und weitere Beschränkungen für die Verwendung biometrischer Daten, die sich aus den nationalen Rechtsvorschriften der Mitgliedstaaten ergeben, lässt die vorliegende Stellungnahme ebenfalls unberührt.[9]

7) Keine Schlussfolgerung in der vorliegenden Stellungnahme greift weiteren technologischen Entwicklungen vor.

8) In der vorliegenden Stellungnahme werden vier Szenarien untersucht, deren spezifische Merkmale in Abschnitt 3.2 beschrieben werden. Andere Szenarien werden nicht behandelt, selbst wenn die Verarbeitung zu denselben Zwecken erfolgt.

[9] In Artikel 9 Absatz 4 DSGVO ist beispielsweise festgelegt, dass die Mitgliedstaaten weitere Bedingungen für die Verarbeitung biometrischer Daten, einschließlich Beschränkungen, beibehalten oder einführen können.

14. In ihrem Antrag wies die französische Aufsichtsbehörde darauf hin, dass die Verarbeitung biometrischer Daten der Fluggäste zum Zweck der Straffung des Fluggaststroms auf Flughäfen auf der Annahme beruht, dass die Einzelpersonen in eine solche Verarbeitung einwilligen, was möglicherweise die Rechtsgrundlage nach der DSGVO bilden würde.[10] **Die Analyse der anwendbaren Rechtsgrundlage fällt jedoch nicht in den Anwendungsbereich der Fragen, die dem EDSA im Antrag vorgelegt wurden. Daher wird die Gültigkeit der Einwilligung in eine solche Verarbeitung gemäß den Artikeln 6, 7 und 9 DSGVO in der vorliegenden Stellungnahme nicht geprüft.**

15. Dennoch stellt der EDSA allgemein fest, dass die betreffenden Verantwortlichen eine gültige ausdrückliche Einwilligung[11] der Einzelpersonen einholen müssten, die mit einer Nutzung dieser Dienste einverstanden sind, wenn sie sich auf diese Rechtsgrundlage stützen. Eine solche ausdrückliche Einwilligung müsste freiwillig, für den konkreten Fall und in Kenntnis der Sachlage[12] erteilt werden, und es würde im Einzelfall geprüft, ob diese Bedingungen erfüllt sind. Unter anderem heißt das:

    1) Einzelpersonen müssten die Möglichkeit haben, diese Einwilligung jederzeit und ohne Nachteile zu widerrufen.[13]

    2) Damit die Einwilligung freiwillig erteilt wird, kann der Einsatz biometrischer Technologien nur auf freiwilliger Basis erfolgen, da Einzelpersonen frei entscheiden können sollten, ob sie mit der Nutzung dieser Dienste einverstanden sind oder nicht, und zwar ohne Nachteile (z. B. deutlich längere Verzögerungen für Fluggäste, die nicht einwilligen)[14], Anreize, zusätzliche Kosten oder zusätzliche Vorteile im Gegenzug.[15]

    3) Von Einzelpersonen, deren biometrische Daten verarbeitet werden, müsste ebenfalls eine ausdrückliche Zustimmung eingeholt werden, auch wenn sie sich nicht zur Identifizierung oder Authentifizierung durch solche Methoden registriert haben. Anders gesagt ist es von wesentlicher Bedeutung, dass die Gesichter von Einzelpersonen, die nicht ausdrücklich in die Gesichtserkennung für den beabsichtigten Zweck eingewilligt haben, nicht von Kameras gescannt werden. Dies kann beispielsweise dadurch erreicht werden, dass bestimmte Kontrollspuren für die Gesichtserkennung vorgesehen werden, und eine angemessene Beschilderung und eine physische Trennung gegenüber den Spuren ohne biometrische Kontrolle

[10] Antrag, Anhang I.

[11] Nach Artikel 4 Absatz 14 und Artikel 9 Absatz 1 DSGVO sowie Artikel 9 Absatz 2 Buchstabe a DSGVO ist die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person untersagt. Dies gilt nicht für den Fall, dass die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat, es sei denn, das Verbot nach Artikel 9 Absatz 1 DSGVO kann gemäß Unionsrecht oder dem Recht der Mitgliedstaaten nicht durch die Einwilligung der betroffenen Person aufgehoben werden. Siehe auch Erwägungsgründe 51, 52 und 53 DSGVO.

[12] Artikel 4 Absatz 11 und Artikel 7 DSGVO.

[13] Artikel 7 Absatz 4 DSGVO, auch Erwägungsgrund 50 DSGVO.

[14] In diesem Zusammenhang könnte z. B. auch darüber nachgedacht werden, wie sich ein System gestalten lässt, mit dem vermieden wird, dass Fluggäste, die nicht einwilligen möchten, sozialem Druck ausgesetzt werden, weil sich ihre Wahl negativ auf andere Fluggäste auswirkt.

[15] EDSA-Leitlinien 05/2020 zur Einwilligung gemäß der Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020 (im Folgenden „**EDSA-Leitlinien 5/2020 zur Einwilligung**“), Rn. 46 und 48.

angebracht werden, um eine eindeutige Identifizierung solcher Kontrollspuren zu ermöglichen.

4) Unbeschadet der Frage, ob die Einwilligung die anwendbare Rechtsgrundlage für eine solche Verarbeitung wäre, gelten die in Artikel 5 DSGVO verankerten Grundsätze der Verarbeitung im Hinblick auf Notwendigkeit und Verhältnismäßigkeit auch dann, wenn Einzelpersonen ihre ausdrückliche Einwilligung zur Verwendung ihrer biometrischen Daten gegeben haben.[16]

16. In dem Antrag wird präzisiert,[17] dass im Hinblick auf die Verarbeitung an den Sicherheitskontrollen des Flughafens die Flughafenbetreiber als Verantwortliche fungieren, während hinsichtlich der Verarbeitung bei der Gepäckaufgabe, beim Boarding und beim Zugang zur Fluggastlounge die Fluggesellschaften die Verantwortlichen sind. Daher stellt der Ausschuss fest, dass verschiedene Akteure an der im Antrag beschriebenen Verarbeitung beteiligt sein können. Die Anwendung der Rollen des (gemeinsam) Verantwortlichen und/oder Auftragsverarbeiters in den in Abschnitt 3.2 der vorliegenden Stellungnahme beschriebenen Szenarien wurde nicht bewertet. In jedem Fall müssen die beteiligten Akteure ermittelt und ihre Zuständigkeiten klar zugewiesen werden, damit die Anforderungen der DSGVO erfüllt sind.[18]

17. Darüber hinaus stellt der Ausschuss fest, dass es in der EU derzeit keine einheitliche rechtliche Verpflichtung für Flughafenbetreiber und Fluggesellschaften im Hinblick darauf gibt, Fluggäste zu identifizieren und an allen genannten Kontrollpunkten zu überprüfen, ob der Name auf der Bordkarte des Fluggastes mit dem Namen auf seinem Identitätsdokument übereinstimmt.[19] Daher unterliegen solche Verpflichtungen nationalen Rechtsvorschriften, die sich von Mitgliedstaat zu Mitgliedstaat unterscheiden können. In einigen Mitgliedstaaten kann eine solche Überprüfung an einigen Kontrollpunkten (z. B. bei der Gepäckaufgabe oder beim Boarding) erforderlich sein, in anderen hingegen sind solche Kontrollen derzeit nicht verpflichtend.[20] Bestehende rechtliche Verpflichtungen zur Überprüfung der Identität der Fluggäste haben unmittelbare Auswirkungen auf die Verfahren der verschiedenen Flughäfen.

---

[16] Ebd., Rn. 5.

[17] Antrag, Anhang I.

[18] Im Einklang mit Artikel 4 Absätze 7 und 8, Artikel 5 Absatz 2 sowie den Artikeln 24, 26, 28 und 29 DSGVO. Siehe auch die EDSA-Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.1, angenommen am 7. Juli 2021.

[19] Die einschlägige Verordnung auf EU-Ebene ist die Durchführungsverordnung (EU) 2015/1998 der Kommission vom 5. November 2015 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit. In dieser Verordnung ist jedoch nicht die Kontrolle amtlicher Ausweispapiere an Kontrollpunkten auf Flughäfen geregelt, und es liegt im Ermessen der Mitgliedstaaten, diese auf nationaler Ebene zu regeln.

[20] Das bedeutet, dass derzeit entweder überhaupt keine Überprüfung durchgeführt oder nur geprüft wird, ob die Bordkarte vorhanden ist. Auf der Grundlage des Protokolls vom 22. Mai 1954 über die Befreiung der Staatsangehörigen Dänemarks, Finnlands, Norwegens und Schwedens von der Verpflichtung, im Besitz eines Reisepasses oder einer Aufenthaltserlaubnis zu sein, während sie ihren Wohnsitz in einem anderen skandinavischen Land als ihrem eigenen haben, sind Staatsangehörige Norwegens, Dänemarks, Finnlands und Schwedens seit dem 1. Juli 1954 von der Verpflichtung befreit, bei Reisen zwischen diesen Ländern im Besitz eines Reisepasses oder eines anderen Ausweises zu sein.

18. Folglich sollte in diesen Fällen, **in denen keine Überprüfung der Identität der Fluggäste anhand eines amtlichen Ausweisdokuments erforderlich ist, keine Überprüfung anhand biometrischer Daten durchgeführt werden, da diese eine übermäßige Datenverarbeitung zur Folge hätte, weil sie im Vergleich zur derzeitigen Situation mit der Verarbeitung zusätzlicher Daten einhergehen und unter Verstoß gegen den Grundsatz der Datenminimierung gemäß Artikel 5 Absatz 1 Buchstabe c DSGVO über das für den betreffenden Zweck notwendige Maß hinausgehen würde**. Diese Erwägung ist bei der Prüfung aller in Abschnitt 3.2 der vorliegenden Stellungnahme beschriebenen Szenarien zu berücksichtigen.

2.2 Schlüsselbegriffe

19. Damit Rohdaten, wie beispielsweise die physischen, physiologischen oder verhaltenstypischen Merkmale einer natürlichen Person, als biometrische Daten im Sinne von Artikel 4 Absatz 14 DSGVO[21] eingestuft werden, muss ihre Verarbeitung mit einer Messung dieser Merkmale einhergehen, da biometrische Daten das Ergebnis solcher Messungen sind.[22]

20. Durch die Verwendung des Abbilds des Gesichts einer Einzelperson (eines Fotos oder Videos), des sogenannten biometrischen „**Samples**“, ist es möglich, eine digitale Darstellung unterschiedlicher Merkmale dieses Gesichts zu extrahieren (das sogenannte „**Template**“).[23] Darüber hinaus weist der Ausschuss noch einmal darauf hin, dass ein „biometrisches Template … eine digitale Darstellung der einzigartigen Merkmale [ist], die aus einem biometrischen Sample extrahiert wurden und in einer biometrischen Datenbank gespeichert werden können“[24], sodass die eindeutige Identifizierung einer natürlichen Person möglich ist oder bestätigt werden kann. Darüber hinaus soll dieses Template „eindeutig und für jeden Menschen spezifisch sein“ und „ist im Prinzip von unbegrenzter zeitlicher Gültigkeit“.[25] In der Regel wird in einem Vergleichsverfahren, das auf die Identifizierung oder Authentifizierung einer Einzelperson mittels Gesichtserkennung abzielt, ein eingehendes biometrisches Template mit gespeicherten Objekten abgeglichen, um entweder zu überprüfen, ob eine Übereinstimmung vorliegt, oder in einer Datenbank eine Übereinstimmung zu finden.[26]

[21] Siehe auch Erwägungsgründe 51, 52 und 53 DSGVO.
[22] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 74.
[23] EDSA-Leitlinien 05/2022 über den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung, Version 2.0, angenommen am 26. April 2023 (im Folgenden „**EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung**“), Rn. 7 und 8.
[24] Ebd., Rn. 9.
[25] Ebd.
[26] EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung, Rn. 10 und 11; siehe auch die Internationale Norm ISO/IEC 2382-37, 2022-03, abrufbar unter: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [letzter Abruf am 23. Mai 2024] (im Folgenden **ISO/IEC 2382-37**).

21. Gesichtserkennungstechnologie kann zwei unterschiedliche Funktionen erfüllen: Authentifizierung[27] und Identifizierung[28]. Es handelt sich zwar um unterschiedliche Funktionen, jedoch stützen sich beide auf die Verarbeitung biometrischer Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen,[29] und fallen daher unter die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO.[30]

22. Insbesondere gilt:

> Bei der **Authentifizierung** soll eine Behauptung, der biometrische Daten zugrunde liegen, durch Abgleich bestätigt werden. In diesem Zusammenhang spricht man auch von „1:1-Überprüfung".
>
> Bei der **Identifizierung** wird eine Datenbank, in der biometrische Daten erfasst sind, mit dem Ziel abgefragt, einer Einzelperson zurechenbare Identifikatoren zu finden. In diesem Zusammenhang spricht man auch von „1-N-Identifizierung".

23. In beiden Fällen (d. h. Identifizierung und Authentifizierung) beruhen die Gesichtserkennungstechniken auf einer geschätzten Übereinstimmung zwischen den Templates, d. h. zwischen dem/den Vergleichs-Templates und dem/den Basis-Templates. Unter diesem Gesichtspunkt sind sie probabilistisch: Aus dem Vergleich wird eine höhere oder geringere Wahrscheinlichkeit im Hinblick darauf abgeleitet, dass es sich bei der Person tatsächlich um die zu authentifizierende oder identifizierende Person handelt. Übersteigt diese Wahrscheinlichkeit einen bestimmten, vom Nutzer oder vom Systementwickler festgelegten Schwellenwert im System, so geht das System davon aus, dass bei der Identifizierung oder Authentifizierung eine Übereinstimmung festgestellt wurde.[31]

[27] Der Ausschuss stellt fest, dass in der künftigen Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz) (noch nicht im Amtsblatt veröffentlicht) die „biometrische Verifizierung" zudem in Artikel 3 Nummer 36 als „die automatisierte Eins-zu-eins-Verifizierung, einschließlich Authentifizierung, der Identität natürlicher Personen durch den Vergleich ihrer biometrischen Daten mit zuvor bereitgestellten biometrischen Daten" definiert wird (siehe legislative Entschließung des Europäischen Parlaments vom 13. März 2024 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[28] Ebenso wird in Artikel 3 Absatz 35 des Gesetzes über künstliche Intelligenz der Begriff „biometrische Identifizierung" als „die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Einzelpersonen, die in einer Datenbank gespeichert sind" definiert.

[29] ISO/CEI 2382-37.

[30] Artikel 4 Absatz 14 DSGVO und EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung, Rn. 12.

[31] EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung, Rn. 11. Siehe auch ISO/IEC 2382-37.

3 BEGRÜNDETHEIT DES ANTRAGS

3.1 Allgemeine Anmerkungen

24. In diesem Abschnitt werden die in Randnummer 4 dargelegten Fragen untersucht. In diesem Zusammenhang wird der Ausschuss für Frage 1 die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstabe f sowie den Artikeln 25 und 32 DSGVO und für Frage 2 die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstaben e und f sowie den Artikeln 25 und 32 DSGVO untersuchen.

25. Zu diesem Zweck untersucht der Ausschuss vier verschiedene Szenarien[32], deren spezifische Merkmale in Abschnitt 3.2 beschrieben werden.

26. Vorab weist der Ausschuss erneut darauf hin, dass die Nutzung biometrischer Daten und insbesondere von Gesichtserkennungstechnologie erhöhte Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringt. Zunächst betrifft die in Rede stehende Verarbeitung biometrische Daten, die nach Artikel 9 DSGVO besonderen Schutz genießen. Insbesondere wird durch biometrische Daten die Verbindung zwischen Körper und Identität auf irreversible Weise geändert, da sie die Merkmale des menschlichen Körpers „maschinenlesbar" machen und deren weitere Verwendung ermöglichen.[33] Darüber hinaus kann der Einsatz von Gesichtserkennungstechnologien mit Risiken in Verbindung mit falschen negativen Ergebnissen, Voreingenommenheit und Diskriminierung einhergehen[34] und das Potenzial für den Missbrauch biometrischer Daten könnte schwerwiegende Auswirkungen auf Einzelpersonen haben, beispielsweise in Form von Identitätsbetrug oder Identitätsfälschung[35]. Es muss auch darauf hingewiesen werden, dass sich die betroffenen Personen dieser Verarbeitung und den damit verbundenen Risiken möglicherweise noch weniger bewusst sind, wenn die Gesichtserkennung aus der Ferne und ohne ihre aktive Beteiligung erfolgt. Schließlich ist zu betonen, dass die Merkmale, auf denen biometrische Daten beruhen, im Allgemeinen als dauerhaft angesehen werden können und als unwiderruflich behandelt werden sollten, insbesondere im Zusammenhang mit der Gesichtserkennung.[36]

27. Selbst wenn derartige Technologien als besonders wirksam angesehen würden, sollten die Verantwortlichen also unter Berücksichtigung der dargelegten Informationen vor deren Einsatz die Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen beurteilen und

---

[32] Die vier vom Ausschuss untersuchten Szenarien beruhen auf den in Anhang I des Antrags aufgeführten Anwendungsfällen. Die französische Aufsichtsbehörde hat klargestellt, dass die in Anhang I des Antrags aufgeführten Anwendungsfälle Umsetzungsbeispiele sind, die zu einem Szenario gehören und zur Veranschaulichung verwendet werden.

[33] Stellungnahme 3/2012 der Artikel-29-Datenschutzgruppe zu Entwicklungen bei biometrischen Technologien, angenommen am 27. April 2012, WP193 (im Folgenden „**Stellungnahme 3/2012 der Artikel-29-DG zu biometrischen Technologien**"), S. 4. In dieser Stellungnahme wird auf die Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („Datenschutzrichtlinie") Bezug genommen. Mit der DSGVO wurde der Anwendungsbereich der besonderen Datenkategorien erweitert, und im Gegensatz zur Datenschutzrichtlinie ist in der DSGVO vorgesehen, dass biometrische Daten zu den besonderen Datenkategorien gehören (Artikel 9 DSGVO).

[34] Guidelines on facial recognition, Beratender Ausschuss des Übereinkommens des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Juni 2021, S. 15; siehe auch EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung, Rn. 27.

[35] Stellungnahme 3/2012 der Artikel-29-DG zu biometrischen Technologien, S. 29.

[36] EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung, Rn. 104.

prüfen, ob sie ihren legitimen Zweck der Verarbeitung mit weniger einschneidenden Mitteln erreichen können.[37]

28. Der Ausschuss weist ferner darauf hin, dass das Recht auf Schutz personenbezogener Daten kein uneingeschränktes Recht ist und unter Wahrung des Grundsatzes der Verhältnismäßigkeit gegen andere durch die Charta geschützte Grundrechte abgewogen werden sollte.[38]

29. In Artikel 25 Absatz 1 DSGVO wird auf die in Artikel 5 DSGVO[39] aufgeführten „Datenschutzgrundsätze" Bezug genommen und vorgeschrieben, dass sie „wirksam"[40] umgesetzt werden. Dies schließt ausdrücklich den Grundsatz der Datenminimierung gemäß Artikel 5 Absatz 1 Buchstabe c DSGVO ein,[41] wonach personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein"[42] müssen. Darüber hinaus wird in Artikel 25 Absatz 2 DSGVO die Verpflichtung zur „standardmäßigen Datenminimierung" festgelegt, die demnach für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit gilt.[43]

30. Artikel 25 DSGVO verpflichtet die Verantwortlichen jedoch nicht, spezifische technische und organisatorische Maßnahmen zu ergreifen, sondern schreibt vielmehr vor, dass die gewählten Maßnahmen und Garantien auf die Umstände und die mit der Verarbeitung verbundenen Risiken für

---

[37] Erwägungsgrund 39 DSGVO. Siehe auch EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 73.

[38] Erwägungsgrund 4 DSGVO. Siehe in diesem Zusammenhang auch Urteil des Gerichtshofs vom 22. Juni 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504 (im Folgenden „C-439/19 Latvijas Republikas Saeima"), Rn. 98, 110 und 113. Darüber hinaus verlangt der Grundsatz der Verhältnismäßigkeit, der zu den allgemeinen Grundsätzen des Unionsrechts gehört, dass die von einem Unionsrechtsakt eingesetzten Mittel zur Erreichung des verfolgten Ziels geeignet sind und nicht über das dazu Erforderliche hinausgehen (siehe Urteil des Gerichtshofs vom 9. November 2010, Volker und Markus Schecke und Eifert, C-92/09 und C-93/09, ECLI:EU:C:2010:662 (im Folgenden „C-92/09 und C-93/09 Volker und Schecke"), Rn. 74 und die dort angeführte Rechtsprechung).

[39] EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20. Oktober 2020 (im Folgenden „**EDSA-Leitlinien 4/2019 zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen**"), Rn. 11.

[40] In Artikel 25 Absatz 1 DSGVO ist Folgendes festgelegt: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen." Siehe EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Rn. 13.

[41] Dementsprechend heißt es in Erwägungsgrund 39 DSGVO, dass personenbezogene Daten nur dann verarbeitet werden sollten, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.

[42] Rechtssache C-439/19 Latvijas Republikas Saeima, Rn. 98; Urteil des Gerichtshofs vom 11. Dezember 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064 (im Folgenden „C-708/18 M5A-ScaraA"), Rn. 48.

[43] EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Rn. 48.

die Rechte und Freiheiten der betroffenen Person abgestimmt sein müssen.[44] Ebenso sieht Artikel 32 DSGVO über die Sicherheit der Verarbeitung vor, dass Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein Schutzniveau zu gewährleisten, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessen ist.

31. Auch wenn Fluggäste ausdrücklich in die Verwendung ihrer biometrischen Daten einwilligen, um den Fluggaststrom auf Flughäfen zu straffen, gelten darüber hinaus die in der DSGVO verankerten Grundsätze der Verarbeitung im Hinblick auf Notwendigkeit und Verhältnismäßigkeit weiterhin und müssen eingehalten werden.[45]

32. Was den **Grundsatz der Notwendigkeit** betrifft, so wird der Ausschuss prüfen, ob die vorgeschlagene Verarbeitung notwendig ist, um das verfolgte Ziel zu erreichen, und ob dasselbe Ziel mit anderen Mitteln, die weniger in die Grundrechte und Grundfreiheiten der betroffenen Person eingreifen, ebenso wirksam erreicht werden kann.[46] Im Hinblick auf den **Grundsatz der Verhältnismäßigkeit** wird der Ausschuss prüfen, ob die negativen Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen in einem angemessenen Verhältnis zu einem erwarteten Nutzen stehen. Ist der Vorteil relativ gering, sind diese Auswirkungen möglicherweise nicht verhältnismäßig.[47]

33. Selbst wenn der Ausschuss der Auffassung ist, dass eines der nachstehend analysierten Szenarien die Anforderungen von Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und Artikel 32 DSGVO erfüllen könnte, obliegt es in jedem Fall dem Verantwortlichen, dies anhand der Sachverhalte nachzuweisen. Für diesen Nachweis sollten auch alternative Szenarien in Betracht gezogen werden.

3.2 Zur Vereinbarkeit mit Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und Artikel 32 DSGVO

3.2.1 Szenario 1: Speicherung des registrierten biometrischen Templates im ausschließlichen Zugriff der Einzelperson zur Authentifizierung

34. In diesem Abschnitt wird untersucht, ob die zur Authentifizierung[48] durchgeführte Speicherung biometrischer Templates von Fluggästen im ausschließlichen Zugriff der Einzelperson, z. B. auf ihrem eigenen Gerät[49], unter ihrer alleinigen Kontrolle[50] (im Folgenden **Szenario 1**) mit Artikel 5 Absatz 1 Buchstabe f sowie den Artikeln 25 und 32 DSGVO vereinbar ist. Außerdem werden in diesem Abschnitt geeignete Garantien für Szenario 1 im Licht der Artikel 25 und 32 DSGVO untersucht.

Beschreibung des Szenarios

35. In Szenario 1 wird das registrierte biometrische Template jedes Fluggastes, der in eine solche Verarbeitung eingewilligt hat, im ausschließlichen Zugriff der Einzelperson gespeichert, z. B. auf einem

[44] EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Rn. 14.
[45] EDSA-Leitlinien 5/2020 zur Einwilligung gemäß Verordnung 2016/679, Rn. 5.
[46] Rechtssache C-439/19, Latvijas Republikas Saeima, Rn. 110 und 113; Urteil des Gerichtshofs (Große Kammer) vom 4. Juli 2023, Meta/Bundeskartellamt, C-252/21, ECLI:EU:C:2023:537, Rn. 108.
[47] C-708/18, M5A-ScaraA, Rn. 52–56, C-92/09 und C-93/09, Volker und Schecke, Rn. 87, C-439/19, Latvijas Republikas Saeima, Rn. 98, 110 und 113. Siehe auch Stellungnahme 3/2012 der Artikel-29-Datenschutzgruppe zu biometrischen Technologien, S. 8.
[48] Siehe Anwendungsfall 1 in Anhang I des Antrags.
[49] Alternativ könnte die Einzelperson ihr biometrisches Template auf Papier ausdrucken und speichern.
[50] Dies gilt unbeschadet der Gesamtverantwortung des für die Verarbeitung Verantwortlichen.

eigenen Gerät, das sich im Besitz und unter der alleinigen Kontrolle des jeweiligen Fluggastes befindet. Die Fluggäste werden authentifiziert (1:1-Abgleich), wenn sie bestimmte Kontrollpunkte auf dem Flughafen passieren.

36. Die Registrierung erfolgt durch den Flughafenbetreiber, entweder per Fernzugriff über die App des Flughafenbetreibers[51] oder an Flughafenterminals mit einem geeigneten Identitätssicherungsniveau (z. B. geeignetes eIDAS-Vertrauensniveau[52]). Diese Registrierung besteht in der Aufzeichnung eines biometrischen Templates und der für die Verarbeitung erforderlichen Identifizierungsdaten[53] (im Folgenden „**Identität**“) auf dem Gerät des Fluggastes. Die Registrierung erfolgt nur einmal für eine bestimmte Gültigkeitsdauer (z. B. entsprechend der Gültigkeitsdauer des Reisepasses des Fluggastes). Weder die Identitäts- noch die biometrischen Daten des Fluggastes werden nach dem Registrierungsverfahren vom Flughafenbetreiber gespeichert.

37. Die Identität und das biometrische Template des Fluggastes werden lokal auf seinem Gerät gespeichert (z. B. in der mobilen App des Flughafenbetreibers oder in einer digitalen Brieftaschen-App). Das Gerät kann dann zur Übermittlung oder Abfrage der Identität und des biometrischen Templates des Fluggastes verwendet werden, gegebenenfalls einschließlich Fluginformationen und/oder der Bordkarte. Diese Informationen werden beispielsweise mit einem Schlüssel verschlüsselt, der sich ausschließlich im Besitz des Flughafenbetreibers befindet – möglicherweise in Form eines QR-Codes, der entweder auf Papier gedruckt oder auf dem Display des Geräts des Fluggastes angezeigt werden kann. In diesem Fall würde der Fluggast diesen QR-Code dann an speziellen Kontrollstationen am Flughafen vorzeigen, die mit einem QR-Scanner und einer Kamera ausgestattet sind.

38. Was die Sicherheit betrifft, so werden die QR-Codes beim Abgleich mit einem Schlüssel entschlüsselt, der sich im Besitz des Flughafenbetreibers befindet, sodass dieser als einziger die QR-Codes entschlüsseln kann. Die biometrischen Daten der Fluggäste werden nur für einen sehr kurzen Zeitraum gespeichert und nach Abschluss des Abgleichs gelöscht. Es ist darauf hinzuweisen, dass Sicherheitsmaßnahmen im Hinblick auf die Speicherung zum Teil von der Sicherheit des Geräts des Fluggastes abhängen.

Bewertung des EDSA

39. Szenario 1 beschreibt technische und organisatorische Maßnahmen, mit denen gemäß Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO ein den Risiken für die betroffenen Personen angemessenes Sicherheitsniveau gewährleistet werden soll. Die Fluggäste werden authentifiziert (1:1-Abgleich), wenn sie bestimmte Kontrollpunkte auf dem Flughafen passieren. In diesem Szenario

[51] Der EDSA stellt fest, dass in Zukunft Alternativen für eine solche Registrierung in Betracht gezogen werden könnten und die Registrierung möglicherweise ohne die App eines bestimmten Flughafenbetreibers erfolgen könnte, beispielsweise durch Interaktion mit der digitalen Brieftasche eines Nutzers.

[52] Ein Rahmen für elektronische Identifizierung und Vertrauensdienste (im Folgenden „**eIDAS**“) auf der Grundlage der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität.

[53] Für die Zwecke dieser Stellungnahme bezeichnet der Begriff „Identifizierungsdaten“ Daten wie Familienname, Vorname, Geburtsdatum usw., die anhand eines Ausweisdokuments oder Reisepasses als zutreffend bestätigt wurden.

erfolgt der Vorgang des Abgleichs hauptsächlich in einer kontrollierten Umgebung[54], wobei die Fluggäste aktiv beteiligt sind und mehr Kontrolle über ihre Daten haben. Vor allem würden nur Fluggäste überprüft, die in eine solche Verarbeitung eingewilligt haben, und die biometrischen Daten anderer Fluggäste, die nicht in eine solche Verarbeitung eingewilligt haben, würden nicht erhoben, sondern ihre Identität würde an speziellen Kontrollstationen geprüft. Darüber hinaus haben die einwilligenden Fluggäste jederzeit die Möglichkeit, die Verarbeitung abzubrechen, indem sie die Daten von ihrem Gerät löschen.

40. Die Verwendung der Gesichtserkennung auf der Grundlage eines biometrischen Templates, das im ausschließlichen Zugriff der Einzelperson gespeichert ist und beispielsweise auf dem eigenen Gerät eines Fluggastes unter seiner alleinigen Kontrolle aufbewahrt wird und über eine spezielle Schnittstelle zur Authentifizierung an bestimmten Kontrollpunkten verwendet werden kann, birgt unter bestimmten Bedingungen geringere Risiken als die Verwendung biometrischer Daten, die in einer zentralen Datenbank gespeichert sind.[55] Geht eine solche lokale Speicherung mit geeigneten Garantien[56] einher, werden die Verletzungen des Schutzes personenbezogener Daten im Vergleich zur zentralen Speicherung abgemildert, wenn es um die Zahl der betroffenen Einzelpersonen geht, und es wird sichergestellt, dass der Zugang zu dem biometrischen Template eine aktive Beteiligung der betroffenen Person voraussetzt.

41. Darüber hinaus könnte der Abgleich vor Ort am Flughafen erfolgen, indem das beispielsweise im QR-Code enthaltene biometrische Template mit der Ausgabe des Templates verglichen wird, das auf der Grundlage des von der Kamera der Kontrollstation erfassten biometrischen Samples berechnet wird. Nur das übereinstimmende Ergebnis würde dem Verantwortlichen, der eine bestimmte Kontrolle durchführt, bekannt gegeben und von ihm verwendet werden (dabei kann es sich entweder um einen Flughafenbetreiber oder eine Fluggesellschaft handeln, je nachdem, ob die Kontrolle an den Sicherheitskontrollen des Flughafens, bei der Gepäckaufgabe, beim Boarding und/oder beim Zugang zur Fluggastlounge erfolgt). Darüber hinaus wirkt die Tatsache, dass die für den Abgleich erforderlichen Informationen (z. B. der QR-Code) von der Einzelperson bereitgestellt werden müssen, als zweiter Faktor[57] und erhöht somit die Sicherheit der Authentifizierung.

42. Mit Blick auf die Vereinbarkeit mit Artikel 25 DSGVO und insbesondere zur Erfüllung der Anforderung der Datenminimierung sollte sichergestellt werden, dass die Verarbeitung dem Grundsatz der Notwendigkeit entspricht. Bei Szenario 1 kann davon ausgegangen werden, dass die gewählten Maßnahmen dem Grundsatz der Notwendigkeit im Hinblick auf den verfolgten Zweck (d. h. Straffung des Fluggaststroms) entsprechen, wenn der Verantwortliche abhängig von den Umständen der Verarbeitung nachweisen kann, dass es keine weniger einschneidenden Alternativlösungen gibt, mit denen dasselbe Ziel wirksam erreicht werden könnte. So könnte der Verantwortliche beispielsweise in der Lage sein, nachzuweisen, dass, auch wenn die Fluggäste ihr Gerät vorzeigen müssten, durch Szenario 1 der Überprüfungsprozess im Vergleich zur aktuellen Situation beschleunigt wird, in der ein

[54] „Unkontrollierte Umgebung“ bezieht sich auf die Verwendung der Gesichtserkennung zur Identifizierung ohne aktive Beteiligung der betroffenen Personen, bei der das Template für die Gesichter aller Personen, die den Überwachungsbereich betreten, mit Templates eines breiten Querschnitts der Bevölkerung verglichen wird, die in einer Datenbank gespeichert sind, siehe EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung, Rn. 17.

[55] EDSA-Leitlinien 5/2022 zur Gesichtserkennung bei der Strafverfolgung, Rn. 17.

[56] Wie in Rn. 46 dargelegt.

[57] Dies mindert beispielsweise das Risiko des Identitätsdiebstahls (Spoofing). Siehe auch Garantie C.1.2.

Mensch überprüft, ob der Name auf der Bordkarte mit dem Identitätsdokument des Fluggastes übereinstimmt.[58] Dies kann insbesondere dann nicht nachgewiesen werden, wenn aktuell keine Kontrollen zur Überprüfung der Identität der Fluggäste anhand ihres amtlichen Ausweisdokuments durchgeführt werden (siehe dazu Rn. 18).

43. Darüber hinaus werden biometrische Templates vom Flughafenbetreiber nach der Registrierung nicht gespeichert, und die Frist für die Speicherung der biometrischen Daten durch den Verantwortlichen, der die Kontrolle durchführt, ist sehr kurz, denn diese Daten werden gelöscht, sobald der Abgleich abgeschlossen ist. Somit begrenzen die in Szenario 1 gewählten Maßnahmen offenbar den Umfang der Verarbeitung und die Speicherfrist der personenbezogenen Daten.

44. Was den Grundsatz der Verhältnismäßigkeit betrifft, so kann die Intensität des Eingriffs, der aus dieser Verarbeitung resultiert, durch die aktive Beteiligung der Fluggäste ausgeglichen werden, da ihre biometrischen Daten in ihrem ausschließlichen Zugriff gespeichert würden. Ferner könnte unter Berücksichtigung der beschriebenen Maßnahmen und unter der Annahme, dass der Verantwortliche angemessene Schutzmaßnahmen anwendet, die für die betreffende Verarbeitung erforderlich sind, die Umsetzung geeigneter Maßnahmen ein dem Risiko angemessenes Sicherheitsniveau gewährleisten. In diesem Fall könnten die negativen Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen als verhältnismäßig zum erwarteten Nutzen angesehen werden.

45. In Anbetracht dieser Ausführungen kommt der Ausschuss in Beantwortung von Frage 1.1 daher zu dem Schluss, dass eine solche Verarbeitung **vorbehaltlich geeigneter Garantien grundsätzlich als mit Artikel 5 Absatz 1 Buchstabe f, Artikel 25 und Artikel 32 DSGVO vereinbar angesehen werden könnte**.

Geeignete Garantien

46. In dieser Art von Szenario vertritt der EDSA in Beantwortung von Frage 1.2 die Auffassung, dass zumindest die folgenden Garantien umgesetzt werden sollten. Es könnten andere als die in dieser Stellungnahme beschriebenen Garantien genutzt werden, um die gleichen Sicherheits- und Datenschutzziele zu erreichen, und sie könnten rechtmäßig sein, solange die Einhaltung des geltenden Rechtsrahmens sichergestellt ist.

47. Hinweis: Dies ist ein allgemeiner und nicht erschöpfender Überblick über die möglichen geeigneten Garantien, die von einem Verantwortlichen in einer mit Szenario 1 vergleichbaren Lösung umgesetzt werden sollten. Ihre Angemessenheit nach den Artikeln 25 und 32 DSGVO unterliegt einer Einzelfallanalyse. Alle Verantwortlichen müssen sicherstellen, dass sie eine eigene Datenschutz-Folgenabschätzung (im Folgenden „DSFA“)[59] vornehmen, und ihre spezifischen Lösungen können zusätzliche Maßnahmen erfordern, die in dieser Stellungnahme nicht enthalten sind.

A. Allgemeines

A.1 Folgenabschätzung für die Datenverarbeitung

[58] Es könnte auch argumentiert werden, dass die biometrische Kontrolle möglicherweise weniger fehleranfällig ist als die Kontrolle durch einen Menschen.
[59] Artikel 35 DSGVO.

A.1.1 Eine Datenschutz-Folgenabschätzung im Einklang mit den Anforderungen von Artikel 35 DSGVO vornehmen, wenn der Verantwortliche einen neuen Verarbeitungsvorgang plant, bei dem eine Verarbeitung mit hoher Wahrscheinlichkeit ein hohes Risiko birgt. Dies dürfte bei Szenario 1 der Fall sein, da es in großem Maßstab die Verarbeitung biometrischer Daten erfordert.[60] Die Angemessenheit der Umsetzung eines Gesichtserkennungssystems während der frühen Entwurfsphase bewerten, einschließlich seiner Notwendigkeit und Verhältnismäßigkeit im Hinblick auf die verfolgten Zwecke,[61] und die Angemessenheit während des gesamten Lebenszyklus der Produktentwicklung überprüfen;

A.1.2 Die zuständige Aufsichtsbehörde konsultieren, falls die Verarbeitung trotz der vom Verantwortlichen zur Risikominderung ergriffenen Maßnahmen weiterhin zu einem hohen Risiko führt.[62]

A.2 Rechte der betroffenen Personen und Garantien, die von den Verantwortlichen umgesetzt werden können

A.2.1 Garantien zur Vermeidung falsch negativer Fälle. Das Risiko von Voreingenommenheit aufgrund von Alter, Geschlecht und Rasse mindern, indem anhand „regelmäßiger Prüfungen … untersucht [wird], ob die Algorithmen zweckentsprechend funktionieren; die Algorithmen werden angepasst, um festgestellte Fehler zu minimieren und die Verarbeitung nach Treu und Glauben zu gewährleisten“[63]. Beispielsweise durch die Einführung menschlicher Aufsicht und Eingriffe, um Voreingenommenheit zu mindern und sicherzustellen, dass im Zusammenhang mit Fluggästen keine Stigmatisierung oder Profilerstellung stattfindet;

A.2.2 Sicherstellen, dass die Verarbeitung personenbezogener Daten transparent abläuft und die Einzelpersonen wissen und kontrollieren können, wie ihre Daten bei jedem Vorgang verarbeitet werden[64];

A.2.3 Maßnahmen zur Einhaltung des Grundsatzes der Zweckbindung sicherstellen, damit die Daten nicht für andere Zwecke genutzt werden, etwa Sicherheits- oder Schulungszwecke;

A.2.4 Sicherstellen, dass keine Fotos oder Videos von Einzelpersonen, die nicht in die Gesichtserkennung eingewilligt haben, erfasst werden, selbst wenn die Fotos oder Videos nicht aufgezeichnet und nicht verarbeitet werden, indem geeignete Maßnahmen getroffen werden (z. B. Verwendung einer angemessenen Fokustiefe und eines angemessenen

[60] Artikel 35 Absatz 3 DSGVO und Leitlinien der Artikel-29-Datenschutzgruppe zur Datenschutz-Folgenabschätzung und zur Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, angenommen am 13. Oktober 2017, WP248rev.01, vom EDSA gebilligt.

[61] Artikel 35 Absatz 7 Buchstabe b DSGVO.

[62] Artikel 36 Absatz 1 DSGVO.

[63] EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Fußnote 60, Rn. 70.

[64] EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Rn. 68 und Erwägungsgrund 7 DSGVO.

Erfassungsbereichs, um zu vermeiden, dass Bilder von anderen Fluggästen im Hintergrund oder in der Umgebung erfasst werden, Einrichtung spezieller Warteschlangen, die in Bezug auf Gesichtserkennung eindeutig gekennzeichnet sind);

A.2.5 Können Kontrollstationen sowohl von Fluggästen, die in die Gesichtserkennung eingewilligt haben, als auch von jenen, die nicht eingewilligt haben, genutzt werden oder können Fluggäste, die nicht in die Gesichtserkennung eingewilligt haben, im Blickfeld erscheinen, während das System nicht genutzt wird, sollte auf eine bestätigende Aktion eines Fluggastes, der eingewilligt hat, gewartet werden, bevor mit der Erfassung des Fotos oder Videos begonnen wird;

A.2.6 Eine betroffene Person sollte die Möglichkeit haben, jederzeit Daten zu löschen, die sich in ihrem ausschließlichen Zugriff befinden (biometrische Templates[65]) und in einer mobilen Anwendung oder digitalen Brieftasche gespeichert sind[66];

A.2.7 Es sollten tragfähige Alternativen oder Ausweichlösungen vorhanden sein (etwa für Fluggäste, die nicht in die Verwendung ihrer biometrischen Daten einwilligen möchten, für Fluggäste, die diese Lösungen nicht nutzen könnten, oder für Fluggäste, bei denen Falschrückweisungen auftreten), um sicherzustellen, dass Fluggäste, die nicht einwilligen, keine Nachteile erleiden[67];

A.2.8 Wird eine Anwendung eingesetzt, sollte sie sorgfältig konzipiert und konfiguriert sein, damit keine unnötigen Daten erhoben werden und die Verwendung von Softwareentwicklungspaketen Dritter, die Daten für andere Zwecke erheben, vermieden wird.

A.3 Rechenschaftspflicht

A.3.1 Bewerten, ob einschlägige Verhaltensregeln oder Zertifizierungsmechanismen vorliegen, die dazu beitragen, die Einhaltung hinsichtlich der Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO nachzuweisen.[68] Überprüfen, ob die Maßnahmen für die betreffende Verarbeitung geeignet sind. Standards[69], bewährte Verfahren und Verhaltenskodizes, die von Verbänden und anderen Gremien, die Kategorien von Verantwortlichen vertreten, anerkannt werden, können bei der Festlegung geeigneter Maßnahmen hilfreich sein;

A.3.2 Grundlegende Sicherheitskontrollen auf dem Gerät des Nutzers gewährleisten, um die Registrierungsphase zu ermöglichen, auch wenn dem Fluggast ebenfalls eine Rolle beim Schutz seiner Daten zukommt, da diese auf seinem Gerät gespeichert sind. Beispiele für solche

[65] Bezugnahmen auf biometrische Templates in den Garantien für Szenario 1 entsprechen Bezugnahmen auf den Schlüssel/das Passwort in Szenario 2.
[66] Es ist zu beachten, dass diese Garantie nur für Szenario 1 gilt.
[67] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 86.
[68] Artikel 32 Absatz 3 DSGVO und EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Rn. 10.
[69] Siehe z. B. ISO/IEC 2382-37.

technischen Prüfungen und Kontrollen sind in Abschnitt C.2 „Infrastruktur und Netzwerk“ aufgeführt.

B. Organisatorisch:

B.1 Strategie und Einhaltung

B.1.1 Sicherstellen, dass interne Zugangskontrollen mit Vorschriften für Administratoren vorhanden sind[70];

B.1.2 Kann der Gesichtserkennungsdienst von einer der an der Verarbeitung beteiligten Parteien ohne Identitäts- oder biometrische Daten oder beide Arten von Daten, die von den jeweils anderen Beteiligten bearbeitet werden müssen, erbracht werden, ist es untersagt, diese Daten über die anderen Parteien zu übermitteln. Beispielsweise muss eine Fluggesellschaft nicht technisch auf die biometrischen Daten zugreifen, wenn sie auf die gemeinsame Flughafeninfrastruktur zurückgreift, selbst wenn diese Fluggesellschaft als Verantwortlicher für die Verarbeitung im Sinne der DSGVO handelt;

B.1.3 Eine Strategie für die Verschlüsselung und das Schlüsselmanagement festlegen[71], etwa für die Verarbeitung der Identitäts- und der biometrischen Daten;

B.1.4 Die Einhaltung der Anforderungen in Kapitel V DSGVO sicherstellen. Beispielsweise konforme Übermittlungen sicherstellen, wenn der Verantwortliche beim Registrierungsverfahren einen Ferndienst in Anspruch nimmt, der seinen Sitz in einem Drittland hat;

B.1.5 Sicherstellen, dass beim Einsatz von Auftragsverarbeitern ein Vertrag[72] mit dem Auftragsverarbeiter im Einklang mit Artikel 28 Absatz 3 DSGVO besteht;

B.1.6 Sicherstellen, dass Verfahren zur Verwaltung menschlicher Aufsicht und Eingriffe vorhanden sind, insbesondere im Hinblick auf den Umgang mit Falschrückweisungen sowie Technik- oder Nutzungsproblemen.

B.2 Schulung und Prüfung

B.2.1. Die ordnungsgemäße Schulung des Personals sicherstellen;

[70] EDSA-Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, angenommen am 21. April 2020 (im Folgenden „**EDSA-Leitlinien 4/2020 zu Standortdaten und Tools zur Kontaktnachverfolgung**“), SEC-10, S. 16.
[71] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 89.
[72] Artikel 28 Absatz 3 DSGVO.

B.2.2 Ein Verfahren „zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“[73] umsetzen;

B.2.3 Ein Verfahren umsetzen, mit dem sichergestellt wird, dass die Verarbeitung des biometrischen Templates[74] des Fluggastes für die Authentifizierung technisch wirksam und hinreichend genau ist;

B.2.4 Sicherstellen, dass die Qualität der biometrischen Samples, die sowohl bei der Registrierung als auch am Kontrollpunkt erfasst werden, ausreicht, um eine zuverlässige biometrische Verarbeitung vorzunehmen.

C. Technisch:

C.1 Zugang

C.1.1 Während der Registrierungsphase Garantien umsetzen, um sicherzustellen, dass der Bootstrap-Registrierungsprozess mit einer überprüften Identität erfolgt. Um beispielsweise die Prüfung der Multifaktor-Authentifizierung der Nutzer zu verbessern, können diverse Maßnahmen umgesetzt werden, von passwortgeschützten Einmal-Links zur Aktivierung der App bis hin zu Mechanismen zur Entsperrung des lokalen Geräts;

C.1.2 Garantien zur Bekämpfung von Falschakzeptanz und Präsentationsangriffen sowie zur Betrugsprävention umsetzen[75];

C.1.3 Der externe Zugriff auf die Identitäts- und die biometrischen Daten ist untersagt[76];

C.1.4 Sicherstellen, dass die Verarbeitung in der Anmelde-, Übermittlungs- und Abgleichphase lokal erfolgt. Der Abgleichpunkt sollte sich so nah wie möglich am Gerät der Einzelperson befinden. Um den Abgleich auf dem einzelnen Gerät zu ermöglichen, könnte eine Interaktion mit Dienstleistern außerhalb des Flughafens erforderlich sein und öffentliche Netzwerkressourcen verwendet werden, mit den Nachteilen, dass es Auswirkungen auf die Verfügbarkeit gäbe und das Template an externe Stellen übermittelt würde;

C.1.5 Einen Nutzer authentifizieren, um einen neuen Flug hinzuzufügen und einen neuen verschlüsselten QR-Code zu generieren;

[73] Artikel 32 Absatz 1 Buchstabe d DSGVO.
[74] Bezugnahmen auf biometrische Templates in den Garantien für Szenario 1 entsprechen Bezugnahmen auf den Schlüssel/das Passwort in Szenario 2.
[75] ENISA Report on Digital Identity on leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust, Januar 2022.
[76] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 89.

C.1.6 Maßnahmen für den Fall umsetzen, dass ein Fluggast den Zugang zu seinem QR-Code verliert.

C.2 Infrastruktur und Netzwerk

C.2.1 Bedingungen für die Aktualisierung des Betriebssystems und die Aktivierung der Authentifizierung für den Zugriff auf das Gerät, damit die Anwendung/digitale Brieftasche funktioniert, einschließlich des automatischen Löschens der Identitäts- und der biometrischen Daten, wenn das Betriebssystem veraltet ist und Sicherheitsrisiken birgt;

C.2.2 Die Abgleichgeräte (d. h. Kontrollstationen) im Betrieb vom Netzwerk isolieren und alle anderen zur Gewährleistung der Sicherheit erforderlichen Maßnahmen treffen;

C.2.3 Den biometrischen Abgleich auf dem Gerät des Fluggastes oder an der Kontrollstation vornehmen (Edge-Computing);

C.2.4 Lösungen zur Behebung von Sicherheitslücken auf individuellen Geräten der Fluggäste, einschließlich der Verschlüsselung von (zumindest) biometrischen Daten und Identitätsdaten im Ruhezustand;

C.2.5 Für (zumindest) biometrische Daten im ausschließlichen Zugriff des Nutzers einen sicheren Speicher verwenden[77], z. B. durch Nutzung eines gesicherten Bereichs auf einem Smartphone;

C.2.6 Sicherheitsmaßnahmen zur Gewährleistung der physischen Sicherheit der Räumlichkeiten, einschließlich des Biometrie-Terminals auf dem Flughafen. Ein hohes Sicherheitsniveau für die Infrastrukturen sicherstellen, mit denen Identitäts- und biometrische Daten verarbeitet werden (z. B. Berechnung, Datenübertragung, vorübergehende oder langfristige Speicherung).

C.3 Sicherheit und Verwaltung der Daten für die Prüfung der Identität der Nutzer

C.3.1 Die Daten während der Übermittlung und Speicherung in mindestens drei verschiedene Gruppen unterteilen, z. B.: Identitätsdaten, biometrische Daten und Flugdaten.[78] Eine angemessene Verschlüsselung der Daten von der Übermittlung bis zur Speicherung sicherstellen;

C.3.2 Technische Maßnahmen umsetzen, um sicherzustellen, dass nur die Daten, die an bestimmten Kontrollpunkten rechtmäßig verarbeitet werden können, am Kontrollpunkt verarbeitet und überprüft werden;

[77] Bezugnahmen auf biometrische Templates in den Garantien für Szenario 1 entsprechen Bezugnahmen auf den Schlüssel/das Passwort in Szenario 2.
[78] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 89.

C.3.3 Die Wirksamkeit der Datenlöschung[79] durch ein sicheres Löschverfahren (z. B. Hauptspeicher, Cache, potenzielle Backups) sicherstellen und den Zeitpunkt, zu dem Daten automatisiert gelöscht werden sollten, bewerten. Die Speicherfristen der Daten sollten durch automatische Verfahren streng durchgesetzt werden, ohne dass eine zusätzliche Maßnahme seitens der Einzelperson erforderlich ist[80];

C.3.4 Die Authentizität und Integrität der Daten (z. B. Signatur) sicherstellen[81];

C.3.5 Die biometrischen Daten der Fluggäste am Registrierungs- und Kontrollpunkt nur sehr kurz speichern und löschen, sobald der Fluggast den Kontrollpunkt durchlaufen hat;

C.3.6 Wird für die Registrierung eine Anwendung verwendet, sollten bei der Entwicklung der Anwendung sowie bei Sicherheitstests durch Dritte Sicherheitsstandards für die Sicherheit mobiler Anwendungen zum Einsatz kommen;

C.3.7 Während der Registrierungsphase am Flughafen Sicherheitsmaßnahmen gewährleisten, um die Vertraulichkeit und Integrität der biometrischen Daten des Fluggastes zu wahren. Wird beispielsweise am Terminal der QR-Code ausgedruckt, sollte er nicht auf dem Terminal angezeigt werden, damit kein böswilliger Akteur ein Foto davon aufnehmen kann. Im Falle einer Nahbereichsübermittlung sollte die Übermittlung unter aktiver Beteiligung des Nutzers und über einen Kanal, der die Nähe sicherstellt, erfolgen;

C.3.8 Daten im ausschließlichen Zugriff der Einzelperson[82] sollten in einem sicheren Speicherbereich auf dem Gerät der Person gespeichert werden, und etwaige Schwachstellen im Zusammenhang mit den Betriebssystemen des Geräts müssen den entsprechenden Sicherheits-Patches unterzogen werden. Im Falle eines gedruckten QR-Codes sollte die Einzelperson darauf hingewiesen werden, dass die darin enthaltenen Daten besonders sensibel sind und wozu er ihn nutzen kann;

C.3.9 Sicherstellen, dass die Registrierung nach angemessenen Verfahren zur Fernidentitätsprüfung[83] erfolgt.

3.2.2 Szenario 2: zentrale Speicherung eines registrierten biometrischen Templates in verschlüsselter Form in den Einrichtungen des Flughafens und mit einem Schlüssel/Passwort im ausschließlichen Zugriff der Fluggäste, zur Authentifizierung

[79] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 89.
[80] EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Rn. 82.
[81] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 89.
[82] Bezugnahmen auf biometrische Templates in den Garantien für Szenario 1 entsprechen Bezugnahmen auf den Schlüssel/das Passwort in Szenario 2.
[83] Siehe ENISA Report on Remote ID Proofing: Analysis of methods to carry out identity proofing remotely, März 2021.

48. In diesem Abschnitt wird die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstaben e und f sowie den Artikeln 25 und 32 DSGVO für den Fall untersucht, dass die zur Authentifizierung durchgeführte zentrale Speicherung der registrierten biometrischen Templates von Fluggästen in einer zentralen Datenbank in verschlüsselter Form und mit einem ausschließlich im Zugriff des Fluggastes befindlichen Schlüssel/Passwort[84] (im Folgenden **Szenario 2**) erfolgt. Außerdem werden in diesem Abschnitt geeignete Garantien für Szenario 2 im Lichte der Artikel 25 und 32 DSGVO untersucht.

Beschreibung des Szenarios

49. In Szenario 2 erfolgt die Registrierung nur einmal für eine bestimmte Gültigkeitsdauer (z. B. ein Jahr nach dem letzten Flug, bis zum Ablauf der Gültigkeit des Reisepasses), entweder per Fernzugriff mit einem geeigneten Identitätssicherungsniveau (z. B. geeignetes eIDAS-Vertrauensniveau) oder an Flughafenterminals. Die Registrierung wird vom Flughafenbetreiber kontrolliert und umfasst die Generierung von Identitäts- und biometrischen Daten, die mit einem Schlüssel/Passwort verschlüsselt werden.

50. Die Datenbank wird in den Räumlichkeiten des Flughafens unter der Kontrolle des Flughafenbetreibers gespeichert. Individuelle Verschlüsselungsschlüssel/-passwörter werden ausschließlich auf dem Gerät der Einzelperson gespeichert (z. B. in der mobilen App des Flughafenbetreibers). Die App kann einen QR-Code mit dem Schlüssel/Passwort erzeugen, der entweder auf Papier ausgedruckt oder auf dem Bildschirm des Geräts angezeigt werden kann.[85] Darüber hinaus erzeugt der Flughafenbetreiber eine zweite Verschlüsselungsebene[86] mit Schlüsseln, die von ihm kontrolliert werden.

51. Die Fluggäste werden authentifiziert (1:1-Abgleich), wenn sie bestimmte Kontrollpunkte auf dem Flughafen passieren. Die Fluggäste, die sich dafür entscheiden, die biometrischen Kontrollpunkte zu passieren, zeigen ihren QR-Code an einer speziellen Kontrollstation vor, die mit einem QR-Scanner und einer Kamera ausgestattet ist. Der Index des Fluggastes wird an die Datenbank gesendet, um das verschlüsselte Template anzufordern, das heruntergeladen und lokal auf der Kontrollstation und/oder dem Gerät des Nutzers überprüft wird. Nur das Ergebnis des Abgleichs ist dem Verantwortlichen des Kontrollpunkts bekannt und wird von ihm verwendet.[87]

52. In diesem Szenario gibt es keine Ströme von Identitäts- und biometrischen Daten zwischen Flughäfen, die zentralen Datenbanken sind nicht miteinander verbunden oder interoperabel.

Bewertung des EDSA

53. In Szenario 2 werden die registrierten biometrischen Templates der Fluggäste zentral gespeichert, jedoch in verschlüsselter Form und mit einem Schlüssel/Passwort, der bzw. das sich im

[84] Siehe Anwendungsfall 2 in Anhang I des Antrags.
[85] Die französische Aufsichtsbehörde hat ferner klargestellt, dass es für die Übermittlung der erforderlichen Informationen auch andere technische Lösungen geben könnte, z. B. die Verwendung eines Protokolls für die Nahbereichskommunikation.
[86] Der Schlüssel/das Passwort selbst (im Zugriff der Einzelperson) wird mit einem anderen Schlüssel verschlüsselt, der sich im Besitz des Flughafenbetreibers befindet.
[87] Die französische Aufsichtsbehörde stellte klar, dass diese Speicherfrist der Veranschaulichung dient und als annehmbar angesehen werden könne, da sich der Schlüssel im Zugriff der Einzelpersonen befindet und in der Registrierungsphase ausgewählt werden kann. Es ist jedoch darauf hinzuweisen, dass diese Speicherfrist angepasst werden kann.

ausschließlichen Zugriff der Fluggäste befindet. Die Fluggäste werden in Szenario 2 authentifiziert (1:1-Abgleich).

54. In diesem Szenario wird vorgeschlagen, dass das Ziel der Straffung des Fluggaststroms (d. h. die Erhöhung der Kontrollgeschwindigkeit) mit einem zentralisierten System erreicht werden könnte. Der EDSA hat bereits festgestellt, dass eine solche Lösung als tragfähige Alternative zur dezentralen Speicherung der registrierten biometrischen Templates[88] (wie in Szenario 1 beschrieben) angesehen werden könnte, wenn objektive Erfordernisse vorliegen und geeignete Garantien angewandt werden (siehe die in Rn. 60 beschriebenen Garantien).

55. Aus Sicherheitsgründen werden die Daten jeder Einzelperson mit dem spezifischen Schlüssel verschlüsselt, der nur von dieser Person und unter ihrer alleinigen Kontrolle aufbewahrt wird. Darüber hinaus wirkt die Tatsache, dass die für den Abgleich erforderlichen Informationen (d. h. der Schlüssel/das Passwort) von der Einzelperson bereitgestellt werden müssen, als zweiter Faktor[89] und erhöht somit die Sicherheit der Authentifizierung. Darüber hinaus erzeugt der Flughafenbetreiber eine zweite Verschlüsselungsebene mit Schlüsseln, die von ihm kontrolliert werden. In Szenario 2 wird der Index der Einzelperson an die zentrale Datenbank gesendet, um die mit der Person verbundenen biometrischen Daten abzurufen. Diese Daten werden dann (verschlüsselt) an einen Computer an dem Kontrollpunkt gesendet, an dem sie zur Durchführung des Abgleichs entschlüsselt werden. Nur das Ergebnis des Abgleichs ist dem Verantwortlichen des Kontrollpunkts bekannt und wird von ihm verwendet. Sofern der Schlüssel/das Passwort der Einzelperson in dem am Kontrollpunkt befindlichen Computer aufbewahrt wird und ausschließlich der Index eines Fluggastes an die zentrale Datenbank gesendet wird, um das verschlüsselte biometrische Template wiederzuerlangen, könnten solche Sicherheitsmaßnahmen als mit Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO vereinbar angesehen werden.

56. Mit Blick auf die Vereinbarkeit mit Artikel 25 DSGVO und insbesondere zur Erfüllung der Anforderung der Datenminimierung sollte sichergestellt werden, dass die Verarbeitung dem Grundsatz der Notwendigkeit entspricht. Bei Szenario 2 kann davon ausgegangen werden, dass die gewählten Maßnahmen dem Grundsatz der Notwendigkeit im Hinblick auf den verfolgten Zweck (d. h. Straffung des Fluggaststroms an Flughäfen) entsprechen, wenn der Verantwortliche abhängig von den Umständen der Verarbeitung nachweisen kann, dass es keine weniger einschneidenden Alternativlösungen gibt, mit denen dasselbe Ziel wirksam erreicht werden könnte. In Szenario 2 müssten die Fluggäste weiterhin ihr Gerät vorzeigen.[90] Der Verantwortliche könnte jedoch in der Lage sein, nachzuweisen, dass mit Szenario 2 der Überprüfungsprozess im Vergleich zur aktuellen Situation, in der ein Mensch überprüft, ob der Name auf der Bordkarte mit dem Identitätsdokument des Fluggastes[91] übereinstimmt, oder im Vergleich zu Szenario 1 beschleunigt wird. Dies kann insbesondere dann nicht nachgewiesen werden, wenn aktuell keine Kontrollen zur Überprüfung der

[88] EDSA-Leitlinien 3/2019 zu Videogeräten, Rn. 88.
[89] Dies mindert beispielsweise das Risiko des Identitätsdiebstahls (Spoofing). Siehe auch Garantie C.1.2.
[90] Die französische Aufsichtsbehörde hat ferner klargestellt, dass es auch andere Optionen für die Vorlage eines Templates geben könnte, z. B. auf Papier. Darüber hinaus nimmt der EDSA zur Kenntnis, dass in Zukunft in Betracht gezogen werden könnte, eine alternative Technologie zu nutzen, z. B. auf der Grundlage eines Nahfeldkommunikations-Systems.
[91] Es könnte auch argumentiert werden, dass die biometrische Kontrolle möglicherweise weniger fehleranfällig ist als die Kontrolle durch einen Menschen.

Identität der Fluggäste anhand ihres amtlichen Ausweisdokuments durchgeführt werden (siehe dazu Rn. 18).

57. Was den Grundsatz der Verhältnismäßigkeit betrifft, so kann die Intensität des Eingriffs, der aus dieser Verarbeitung resultiert, durch die aktive Beteiligung der Fluggäste ausgeglichen werden, die den Schlüssel zu ihren verschlüsselten Daten unter ihrer alleinigen Kontrolle halten. Darüber hinaus lassen sich die Sicherheitsrisiken, die sich daraus ergeben, dass die biometrischen Daten der Fluggäste in einer zentralen Datenbank gespeichert werden und sich der Schlüssel im ausschließlichen Zugriff der Fluggäste befindet, offenbar durch geeignete Garantien mindern (siehe Rn. 60). Unter der Annahme, dass der Verantwortliche die geeigneten Garantien, die für die betreffende Verarbeitung erforderlich sind, anwendet, könnten daher die Risiken für Einzelpersonen gemindert und die negativen Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen mit Blick auf den erwarteten Nutzen als verhältnismäßig angesehen werden. Natürlich sollte in jedem Fall sichergestellt werden, dass ausschließlich die für den Zweck erforderlichen Daten verarbeitet und nur die Fluggäste, die eingewilligt haben, überprüft werden, sodass keine Gefahr besteht, dass biometrische Daten anderer Fluggäste, die nicht eingewilligt haben, erhoben werden.

58. Als Beispiel wird im Antrag angeführt, dass in Szenario 2 die Speicherfrist der verschlüsselten Daten in der Datenbank üblicherweise ein Jahr nach dem letzten Flug der Einzelperson und bis zum Ablauf der Gültigkeit des Reisepasses betragen könnte. In dem Antrag wurden keine Informationen zur Rechtfertigung eines derart langen Zeitraums mit objektiven Gründen vorgelegt, es kann jedoch davon ausgegangen werden, dass eine solche Speicherfrist aus Gründen der Bequemlichkeit für künftige Flüge vorgesehen ist. Um in diesem Szenario mit Blick auf die Speicherfrist die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstabe e DSGVO zu erreichen, sollten die Verantwortlichen begründen können, warum in bestimmten Fällen die Speicherfrist für den Zweck erforderlich ist. Der Ausschuss empfiehlt den Verantwortlichen, eine möglichst kurze Speicherfrist vorzusehen und dabei auch Fluggäste zu berücksichtigen, die nur sehr selten fliegen, und den betroffenen Personen anzubieten, die von ihnen bevorzugte Speicherfrist festzulegen.

59. In Anbetracht dieser Ausführungen kommt der Ausschuss in Beantwortung von Frage 2.1.1 zu dem Schluss, dass eine solche Verarbeitung **vorbehaltlich geeigneter Garantien grundsätzlich als mit Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und Artikel 32 DSGVO vereinbar angesehen werden könnte**.

Geeignete Garantien

60. Bei dieser Art von Szenario vertritt der Ausschuss in Beantwortung der Frage 2.1.2 die Auffassung, dass **zusätzlich zu den in Szenario 1 aufgeführten Garantien** zumindest die folgenden Garantien umgesetzt werden sollten. *Es könnten andere als die in dieser Stellungnahme beschriebenen Garantien genutzt werden, um die gleichen Sicherheits- und Datenschutzziele zu erreichen, und sie könnten rechtmäßig sein, solange die Einhaltung der geltenden Rechtsrahmen sichergestellt ist.*

61. Hinweis: *Dies ist ein allgemeiner und nicht erschöpfender Überblick über die möglichen geeigneten Garantien, die von einem Verantwortlichen in einer mit Szenario 2 vergleichbaren Lösung umgesetzt werden könnten. Ihre Angemessenheit nach den Artikeln 25 und 32 DSGVO unterliegt einer Einzelfallanalyse. Alle Verantwortlichen müssen sicherstellen, dass sie eine eigene Datenschutz-Folgenabschätzung vornehmen, und ihre spezifischen Lösungen können zusätzliche Maßnahmen erfordern, die in dieser Stellungnahme nicht enthalten sind.*

D. Allgemeines

D.1 Rechte der betroffenen Personen und Garantien, die von den Verantwortlichen umgesetzt werden können

D.1.1 Die Kontrolle des Fluggastes über die Datenspeicherfristen für alle seine Daten sicherstellen. Die Speicherfristen sollten auf das für den spezifischen Zweck erforderliche Maß begrenzt werden. Ausgehend von einer gründlichen Analyse von Faktoren wie der Gültigkeit des Ausweises sollte eine Höchstdauer festgelegt werden. Den betroffenen Personen sollte angeboten werden, die von ihnen bevorzugte Speicherfrist festzulegen, die kürzer als die Standardspeicherfrist sein könnte;

D.1.2 Eine betroffene Person sollte die Möglichkeit haben, jederzeit das Löschen der Daten zu fordern, die sich in ihrem ausschließlichen Zugriff befinden (Schlüssel/Passwort) und in einer mobilen Anwendung oder digitalen Brieftasche gespeichert sind[92];

D.1.3 Sicherstellen, dass der Standort der zentralen Datenbank eine wirksame Aufsicht durch die zuständige Aufsichtsbehörde ermöglicht.

E. Organisatorisch:

E.1 Strategie und Einhaltung

E.1.1 Das Vertrauen in den zentralen Server muss begrenzt werden. Es muss sichergestellt werden, dass die Verwaltung des zentralen Servers klar definierten Governance-Regeln folgt und alle erforderlichen Maßnahmen zur Gewährleistung seiner Sicherheit umfasst.[93]

F. Technisch:

F.1 Zugang

F.1.1 Protokolle über die Personen führen, die Zugang zu personenbezogenen Daten haben, insbesondere zu Identitäts- und biometrischen Daten, sowie über die Zugriffszeitpunkte;

F.2 Infrastruktur und Netzwerk

F.2.1 Die zentrale Datenbank angemessen schützen, auch vor Verfügbarkeitsangriffen;

F.2.2 Sicherstellen, dass die zentrale Datenbank, die Registrierungsstationen und die Abgleichgeräte nicht mit dem Internet verbunden sind. Der Betrieb und die Wartung

[92] Es ist darauf hinzuweisen, dass diese Garantie nur für Szenario 2 gilt.
[93] EDSA-Leitlinien 4/2020 zu Standortdaten und Tools zur Kontaktnachverfolgung, PRIV-5, S. 17.

dieses Systems (z. B. Sicherung, Patching, Überwachung usw.) sind lokal in den Räumlichkeiten des Flughafens durchzuführen.

F.3 Datensicherheit und Datenverwaltung

F.3.1 Kryptografische Techniken nach dem neuesten Stand der Technik umsetzen, um den Austausch zwischen der Anwendung und dem zentralen Server sicherzustellen[94];

F.3.2 Den individuellen Schlüssel/das individuelle Passwort auf der Ebene aufbewahren, auf der er bzw. es zur Entschlüsselung verwendet wird (d. h. auf der Kontrollstation), und den Index ausschließlich verwenden, um das entsprechende biometrische Template in der zentralen Datenbank wiederzuerlangen;

F.3.3 Sicherstellen, dass beim Austausch des Schlüssels/des Passworts zwischen dem Benutzergerät und der Kontrollstation, die Kommunikation vor jeglichem möglichen Abhören oder einer Übermittlung an Dritte geschützt ist;

F.3.4 Das biometrische Template bei Speicherung in der zentralen Datenbank indexieren, um eine 1:1-Authentifizierung zu ermöglichen und sicherzustellen, dass es eindeutig ist und sich auf die Einzelperson bezieht. Es ist sicherzustellen, dass der Index keine der Identitätsinformationen des Fluggastes offenbart und nicht mit dem Verschlüsselungsschlüssel zusammenhängt;

F.3.5 Alle Übermittlungen zwischen der zentralen Datenbank und den Kontrollpunkten angemessen authentifizieren und verschlüsseln und über isolierte Netzwerke durchführen;

F.3.6 Bidirektionale Verbindungen zwischen Datensätzen (Identitäts- und biometrischen Daten sowie Flugdaten) vermeiden und nur relevante unidirektionale Verbindungen in der Datenbank aufbewahren. Beispielsweise nur die unidirektionalen Verbindungen vom Index zu Identitätsdaten, vom Index zu verschlüsselten biometrischen Daten und vom Index zu Flugdaten;

F.3.7 Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs treffen, z. B. durch geeignete Backup-Speichersysteme;

F.3.8 Sicherstellen, dass auf den Kontrollstationen keine Protokolle über verschlüsselte oder unverschlüsselte Templates geführt werden.

[94] EDSA-Leitlinien 4/2020 zu Standortdaten und Tools zur Kontaktnachverfolgung, SEC-4, S. 16: „Eingesetzt werden können beispielsweise folgende Techniken: Symmetrische und asymmetrische Verschlüsselung, Hash-Funktionen, Protokolle wie Private Membership Test und Private Set Intersection, Bloom-Filter, Private Information Retrieval, homomorphe Verschlüsselung usw.“

3.2.3 Zentrale Speicherung der registrierten biometrischen Templates für die Identifizierung

62. In diesem Abschnitt wird die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstaben e und f sowie den Artikeln 25 und 32 DSGVO für den Fall untersucht, dass für die Identifizierung eine zentrale Speicherung der registrierten biometrischen Templates der Fluggäste erfolgt, wobei diese Templates nicht mit einem ausschließlich im Zugriff des Fluggastes befindlichen Schlüssel/Passwort verschlüsselt werden. Dies geschieht anhand zweier Anwendungsfälle: 1. wenn solche Templates in einer Datenbank in den Einrichtungen des Flughafens unter der Kontrolle des Flughafenbetreibers gespeichert werden[95] (im Folgenden **Szenario 3.1**) und 2. wenn solche Templates in der Cloud unter der Kontrolle der Fluggesellschaft gespeichert werden[96] (im Folgenden **Szenario 3.2**).

63. Der Ausschuss ist der Auffassung, dass die Verwendung biometrischer Daten zum Zweck der **Identifizierung** in großen zentralen Datenbanken die Grundrechte der betroffenen Personen beeinträchtigt und möglicherweise schwerwiegende Folgen für die betroffenen Personen haben könnte.[97] Darüber hinaus sollte die Verwendung biometrischer Daten auch unter Berücksichtigung der Grundsätze der Notwendigkeit und Verhältnismäßigkeit im Hinblick auf den Zweck, für den sie verarbeitet werden, geprüft werden.[98]

3.2.3.1 Szenario 3.1: zentrale Speicherung in einer Datenbank in den Einrichtungen des Flughafens unter der Kontrolle des Flughafenbetreibers

Beschreibung des Szenarios

64. In Szenario 3.1 wird das registrierte biometrische Template der Fluggäste in verschlüsselter Form in einer zentralen Datenbank in den Räumlichkeiten des Flughafens und unter der Kontrolle des Flughafenbetreibers gespeichert. Insbesondere sind die Fluggastdaten unterteilt, d. h. ihre Identitätsdaten, das registrierte biometrische Template und die Fluginformationen werden in drei verschiedenen Datenbanken gespeichert. Diese Daten werden mit unterschiedlichen Schlüsseln verschlüsselt, und zwar sowohl während der Speicherung als auch der Übermittlung an die Server, die den Abgleich durchführen; dort werden die Daten anschließend vom Flughafenbetreiber entschlüsselt.

65. Die Fluggäste müssen sich innerhalb eines kurzen Zeitraums vor ihrem Abflug (z. B. 48 Stunden) für den jeweiligen Flug registrieren. Diese Registrierung kann entweder per Fernzugriff oder an Flughafenterminals mit einem geeigneten Identitätssicherungsniveau (z. B. geeignetes eIDAS-Vertrauensniveau) erfolgen. Alternativ kann die Registrierung in derselben Form erfolgen wie in Szenario 1 beschrieben; in diesem Fall müssen die Fluggäste ihre Daten innerhalb von 48 Stunden vor ihrem Abflug von ihren digitalen Brieftaschen in das Flughafensystem übertragen.

---

[95] Siehe Anwendungsfall 3A in Anhang I des Antrags.
[96] Siehe Anwendungsfall 3B in Anhang I des Antrags.
[97] Siehe z. B. Stellungnahme 3/2012 der Artikel-29-Datenschutzgruppe zu biometrischen Technologien, S. 8. Siehe auch Rn. 26.
[98] Erwägungsgrund 4 DSGVO. Siehe auch Stellungnahme 3/2012 der Artikel-29-Datenschutzgruppe zu biometrischen Technologien, S. 8.

66. Auch in diesem Szenario passieren die Fluggäste eine spezielle Kontrollstation, die mit einer Kamera ausgestattet ist. Ihr biometrisches Sample wird dann an einen zentralen Flughafenserver gesendet, auf dem versucht wird, die Daten mit denen der zentralen biometrischen Datenbank abzugleichen. Der Fluggast kann auf diese Weise identifiziert werden, und es lässt sich überprüfen, ob er tatsächlich für einen abgehenden Flug (oder für das Boarding im Falle einer Kontrolle beim Einsteigen) registriert ist oder nicht. Je nach Kontrollpunkt können die an den abfragenden Verantwortlichen des Kontrollpunkts zurückgeschickten Daten minimiert werden, z. B. könnte als Antwort „Ja" oder „Nein" oder erforderlichenfalls das Abgleichergebnis selbst zurückgemeldet werden. In diesem Fall wird nur das Abfrageergebnis an einen Verantwortlichen des Kontrollpunkts übermittelt und von diesem verwendet.

67. Insbesondere werden in diesem Szenario die Fluggäste identifiziert (1:N-Abgleich), wobei N die Zahl der Fluggäste ist, die in einem Zeitraum von mehreren Tagen am Flughafen erwartet werden. Darüber hinaus wird der biometrische Abgleich nur vorgenommen, wenn sich jeder Fluggast an vorab festgelegten Kontrollpunkten am Abgangsflughafen zeigt, die Datenverarbeitung erfolgt jedoch auf einem zentralen Server, der mit der zentralen Datenbank verbunden ist. In diesem Szenario beträgt die Speicherfrist in der Regel 48 Stunden, und die Daten werden gelöscht, sobald das Flugzeug gestartet ist.

Bewertung des EDSA

68. Wie bereits erwähnt, birgt die Verarbeitung biometrischer Daten erhöhte Risiken für die Rechte und Freiheiten der betroffenen Personen.[99] Ein Fehler bei der Datensicherheit kann daher besonders schwerwiegende Folgen für die betroffenen Personen haben.[100] Die Verantwortlichen sind verpflichtet, diese Risiken wirksam zu mindern. Da in diesem Szenario die gesamte Architektur vollständig zentralisiert ist, verlieren die Fluggäste in größerem Maße die Kontrolle über ihre Daten. Darüber hinaus könnte auch das Risiko größer sein, dass die Daten für andere Zwecke als die Kontrolle des Fluggaststroms verarbeitet werden.

69. Vor dem Hintergrund des Grundsatzes der Sicherheit und der Sicherheitsanforderungen (Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO) sollte berücksichtigt werden, dass die Speicherung von Identitäts- und biometrischen Daten in zentralen, wenn auch getrennten Datenbanken ergiebige Angriffspunkte bieten kann und dass eine Verletzung der Vertraulichkeit einer solchen Datenbank in der Folge einen Zugriff auf den gesamten Datensatz nach sich ziehen kann. Folglich kann eine mögliche Verletzung im Zusammenhang mit Templates für die Gesichtserkennung und den zugehörigen Identitätsdaten die unbefugte oder unrechtmäßige Identifizierung der betroffenen Personen in anderen Umgebungen ermöglichen. Je nach den für die biometrische Identifizierung verwendeten Methoden kann dadurch auch die weitere sichere Verwendung von Gesichtserkennungs-Templates als Identifikator gefährdet werden. In diesem Fall können die Auswirkungen der Verletzung nicht abgemildert werden, anders als bei einer anderen Art von Anmeldeinformationen (z. B. Benutzerkennung, Passwort), die geändert werden können.[101]

[99] Siehe Rn. 26.
[100] Guidelines on facial recognition, Beratender Ausschuss des Übereinkommens des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Juni 2021, S. 22.
[101] Siehe hierzu Stellungnahme 3/2012 der Artikel-29-Datenschutzgruppe zu biometrischen Technologien, S. 34.

70. Ferner machen die hohe Quantität und Qualität der im Besitz des Verantwortlichen gespeicherten Identitäts- und biometrischen Daten diese zu einem sehr wertvollen Ziel für einen Angreifer, woraus sich, im Sinne des Sicherheitsrisikos, eine höhere Eintrittswahrscheinlichkeit ergibt. Ebenfalls könnten Datenschutzverletzungen größere Auswirkungen haben, da es aufgrund der Speicherung von Daten an einem zentralen Ort für Angreifer einfacher sein könnte, auf personenbezogene Daten gleich mehrerer Fluggäste zuzugreifen. Daher könnte eine mögliche Verletzung möglicherweise eine große Zahl betroffener Personen hohen Risiken im Sinne der Schadensschwere aussetzen, z. B. Identitätsdiebstahl in großem Maßstab, die äußerst schwierig zu mindern sind.

71. Was die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO betrifft, reichen daher unter Berücksichtigung des Stands der Technik die in Szenario 3.1[102] vorgesehenen Maßnahmen nicht aus, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Auf dieser Grundlage wäre die Verarbeitung nach Szenario 3.1 mit Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO nicht vereinbar, wenn sich ein Verantwortlicher auf diese Maßnahmen beschränken würde.

72. Vor dem Hintergrund des Grundsatzes von Artikel 5 Absatz 1 Buchstabe e DSGVO beträgt die Speicherfrist biometrischer Daten in der zentralen Datenbank in diesem Szenario in der Regel 48 Stunden. Eine solche Begrenzung der Speicherung verringert die Risiken im Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten offenbar erheblich. Die Speicherfrist ist für sich genommen allerdings kein entscheidender Faktor für die Vereinbarkeit dieser Architektur insgesamt, da die Speicherfristen von den Verantwortlichen geändert werden können. In jedem Fall müssen die vorgeschlagenen Maßnahmen den Anforderungen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 25 DSGVO entsprechen.

73. Im Gegensatz zu den Szenarien 1 und 2, bei denen die Fluggäste authentifiziert werden, werden die Fluggäste in Szenario 3.1 identifiziert (1:N-Abgleich), wobei N die Zahl der Fluggäste ist, die in einem Zeitraum von mehreren Tagen auf dem Flughafen erwartet werden und die in eine solche Verarbeitung beim Passieren bestimmter Kontrollpunkte auf dem Flughafen eingewilligt haben. Das heißt, dass die Fluggäste in einer zentralen Datenbank gesucht werden, indem jedes erfasste biometrische Sample verarbeitet wird, um zu überprüfen, ob es mit einer dem System bekannten Person übereinstimmt. Im Gegensatz zu Szenario 2 befinden sich die Schlüssel in Szenario 3.1 nicht ausschließlich im Zugriff der Fluggäste. Folglich haben die Fluggäste in diesem Szenario deutlich weniger Kontrolle über ihre biometrischen Daten. Daher kann eine solche Verarbeitung, wie sie in Szenario 3.1 vorgeschlagen wird, nicht mit den Anforderungen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 25 DSGVO vereinbar sein.

74. Im Lichte von Artikel 25 DSGVO sollten die Verantwortlichen die Arten, die Kategorien und den Detailgrad der für die Verarbeitungszwecke erforderlichen personenbezogenen Daten berücksichtigen.[103] Bei ihren Gestaltungsentscheidungen sollten die erhöhten Risiken für die Grundsätze der Datenminimierung, Integrität und Vertraulichkeit sowie Speicherbegrenzung im Fall der Erhebung großer Mengen detaillierter personenbezogener Daten berücksichtigt und mit der Risikoverringerung durch die Erhebung kleinerer Mengen und/oder weniger detaillierter

[102] Wie in den Rn. 64–67 beschrieben.

[103] EDSA-Leitlinien 4/2019 zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, Rn. 49.

Informationen über betroffene Personen verglichen werden. In jedem Fall sollte die Standardeinstellung nicht die Erhebung personenbezogener Daten umfassen, die für den spezifischen Verarbeitungszweck nicht erforderlich sind. Sind also bestimmte Kategorien personenbezogener Daten unnötig oder werden keine detaillierten Daten benötigt, weil weniger genaue Daten ausreichen, sollten keine überschüssigen personenbezogenen Daten erhoben werden. Könnte mit einer anderen Verarbeitungsmethode, die wie in Szenario 3.1 beschrieben verfügbar ist, dasselbe Ziel erreicht werden, ist es in diesem Fall nicht erforderlich, Gesichtserkennungstechnologie zu verwenden.

75. Was Artikel 25 DSGVO betrifft, so ist die Autonomie der betroffenen Person ein wesentliches Element des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Vor allem sollte der betroffenen Person bei der Bestimmung der Verwendung ihrer personenbezogenen Daten sowie mit Blick auf den Umfang und die Bedingungen dieser Nutzung oder Verarbeitung das Höchstmaß an Autonomie gewährt werden.[104] In Szenario 1 hätte die betroffene Person Autonomie und Kontrolle im Hinblick auf die Verwendung, Offenlegung und Löschung ihrer biometrischen Templates, und in Szenario 2 behielte die betroffene Person eine gewisse Kontrolle über die Offenlegung ihres eigenen biometrischen Templates, da der Verschlüsselungsschlüssel/das Passwort in ihrem Zugriff gespeichert würde. In Szenario 3.1 ist die betroffene Person hinsichtlich der Verarbeitung ihrer biometrischen Daten jedoch vollständig von den Entscheidungen des Verantwortlichen abhängig und hat daher keine direkte Kontrolle über die Verwendung ihres biometrischen Templates.

76. Mit Blick auf die Vereinbarkeit mit Artikel 25 DSGVO und insbesondere auf die Erfüllung der Anforderung der Datenminimierung kann die in Szenario 3.1 vorgesehene Verarbeitung nicht dem Grundsatz der Notwendigkeit entsprechen. Der Ausschuss ist der Auffassung, dass ein ähnliches Ergebnis im Hinblick auf die Straffung des Fluggaststroms auf Flughäfen in einer weniger in die Privatsphäre eingreifenden Weise erreicht werden kann. Beispielsweise kann dies ohne die Verwendung biometrischer Daten erreicht werden (auch wenn die Nutzererfahrung dann anders wäre, da es möglicherweise länger dauern könnte, die Bordkarte und gegebenenfalls amtliche Ausweisdokumente vorzuzeigen). Darüber hinaus ermöglichen andere Lösungen, die Ziele in einer weniger in die Privatsphäre eingreifenden Weise zu erreichen, insbesondere solche, die sich auf die Speicherung der biometrischen Daten in einer lokalen Brieftasche auf dem Gerät der betreffenden Einzelperson stützen, oder solche, die eine Verschlüsselung der Daten mit einem bestimmten Schlüssel erfordern, der auf dem Gerät der Einzelperson gespeichert ist.

77. Was den Grundsatz der Verhältnismäßigkeit betrifft, so würde die in Szenario 3.1 vorgesehene Verarbeitung Risiken für die Rechte der betroffenen Personen mit sich bringen, die angesichts des Stands der Technik durch die vorgesehenen Garantien nicht gemindert würden. Das Risiko negativer Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen, das sich aus einer Verletzung des Schutzes personenbezogener Daten in einer zentralen Datenbank biometrischer Daten einer großen Zahl von Einzelpersonen ergeben könnte, scheint den erwarteten Nutzen der Verarbeitung zu überwiegen, da dieser Nutzen, d. h. eine leichte Erhöhung des Komforts und der Geschwindigkeit der Kontrollen, relativ gering ist. Daher kann er die hohe Intensität des Eingriffs dieser

[104] EDSA-Leitlinien 4/2019 zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, Rn. 70. In Erwägungsgrund 7 der DSGVO wird weiter klargestellt, dass „[n]atürliche Personen … die Kontrolle über ihre eigenen Daten besitzen [sollten]“.

Maßnahmen in die Grundrechte und Grundfreiheiten der Einzelpersonen nicht rechtfertigen, sodass die in Szenario 3.1 vorgesehene Verarbeitung nicht mit dem Grundsatz der Verhältnismäßigkeit vereinbar ist.

78. In Anbetracht dieser Erwägungen kommt der Ausschuss in Beantwortung der Frage 2.2.1 zu dem Schluss, dass, wenn die Verarbeitung speziell zum Zweck der Straffung des Fluggaststroms auf Flughäfen erfolgt, die in Szenario 3.1 vorgesehene Verarbeitung

- **nicht mit Artikel 25 DSGVO vereinbar sein kann**;
- **Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO nicht entsprechen würde**, wenn sich ein Verantwortlicher auf die in Szenario 3.1 beschriebenen Maßnahmen beschränken würde.

3.2.3.2 Szenario 3.2: zentrale Speicherung in einer Cloud unter der Kontrolle der Fluggesellschaft

Beschreibung des Szenarios

79. In Szenario 3.2 wird das registrierte biometrische Template der Fluggäste unter der Kontrolle der Fluggesellschaft oder ihres Cloud-Diensteanbieters (Auftragsverarbeiter) in der Cloud gespeichert. In dem Antrag wird bestimmt, dass der Cloud-Diensteanbieter seinen Sitz im EWR hätte.[105] In diesem Fall werden die Fluggastdaten verschlüsselt, aber während der Verwendung (z. B. bei der Durchführung des Abgleichs) entschlüsselt, und die Schlüssel befinden sich unter der Kontrolle der Fluggesellschaft oder ihres Cloud-Auftragsverarbeiters. Die biometrischen Daten der Fluggäste werden zur Identifizierung der Fluggäste (1:N-Abgleich) verwendet, wobei N potenziell einem Wert bis zur Gesamtzahl der Kunden der Fluggesellschaft entsprechen kann.[106]

80. Ähnlich wie bei den Szenarien 1, 2 und 3.1 müssen sich die Fluggäste auch hier zunächst registrieren. In Szenario 3.2 erfolgt die Registrierung der Fluggäste jedoch einmal, solange der Kunde über ein Konto bei der Fluggesellschaft verfügt. Die Registrierung erfolgt entweder im Fernmodus mit einem geeigneten Identitätssicherungsniveau (z. B. geeignetes eIDAS-Vertrauensniveau) oder an Flughafenterminals. Der Abgleich biometrischer Daten erfolgt nur dann, wenn die Fluggäste an vorab festgelegten Kontrollpunkten am Flughafen erscheinen, die Datenverarbeitung erfolgt jedoch in der Cloud.

81. Auf dem Flughafen passieren die Fluggäste spezielle Kontrollstationen, die mit einer Kamera ausgestattet sind. Die biometrischen Daten der Fluggäste werden über eine Anfrage an einen Cloud-Server der Fluggesellschaft übermittelt, wo der Abgleich dieser Daten mit der zentralen Datenbank erfolgt. Der Fluggast kann auf diese Weise identifiziert werden, und es lässt sich überprüfen, ob er tatsächlich für einen abgehenden Flug (oder für das Boarding im Falle einer Kontrolle beim Einsteigen) registriert ist oder nicht.

82. Potenziell können die Abgleichergebnisse mehreren Flughafenbetreibern zur Verfügung gestellt werden, wenn eine Fluggesellschaft über ein spezielles Terminal verfügt oder Zugang zur Infrastruktur des gemeinsamen Informationssystems eines Flughafens hat. Je nach Kontrollpunkt können die an den abfragenden Verantwortlichen des Kontrollpunkts zurückgeschickten Daten minimiert werden, z. B. könnte als Antwort „Ja“ oder „Nein“ oder erforderlichenfalls das Abgleichergebnis selbst zurückgemeldet werden. In diesem Fall wird nur das Abfrageergebnis an einen Verantwortlichen des Kontrollpunkts übermittelt und von diesem verwendet.

83. Die Speicherfrist des Templates wird von der Fluggesellschaft festgelegt und kann möglicherweise so lange andauern, wie der Kunde über ein Konto bei der Fluggesellschaft verfügt.

Bewertung des EDSA

[105] Die französische Aufsichtsbehörde stellte klar, dass dies der Veranschaulichung dient und dass auch Cloud-Diensteanbieter in Betracht gezogen werden könnten, die ihren Sitz nicht im EWR haben. Darüber hinaus könnten auch andere Speicherlösungen (z. B. ohne Cloud-Nutzung) in Betracht gezogen werden.

[106] Die französische Aufsichtsbehörde stellte klar, dass dies der Veranschaulichung dient und dass es eine Lösung gibt, bei der biometrische Daten vor jedem Flug übertragen werden.

84. Die Erwägungen, die der Ausschuss bereits zu Szenario 3.1[107] geäußert hat, gelten auch für dieses Szenario.

85. Was den Grundsatz der Sicherheit und die Sicherheitsanforderungen (Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO) betrifft, so erfolgt die Verarbeitung in Szenario 3.2 in der Cloud, und mehrere Einrichtungen, möglicherweise auch Anbieter außerhalb des EWR, könnten Zugang zu diesen Daten haben, auch wenn sich die Daten im EWR befinden.[108] Eine Architektur dieser Art birgt potenzielle Risiken im Hinblick auf die Übermittlung personenbezogener Daten an Drittländer. Ferner werden die Fluggastdaten zwar verschlüsselt, aber bei Verwendung (d. h. bei der Durchführung des Abgleichs) entschlüsselt, wobei sich die Schlüssel unter der Kontrolle der Fluggesellschaft oder ihres Cloud-Auftragsverarbeiters befinden. Eine solche Speicherung kann dazu führen, dass sich die Angriffsfläche für eine Sicherheitsgefährdung weiter vergrößert.

86. Was die Vereinbarkeit mit Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO betrifft, reichen daher unter Berücksichtigung des Stands der Technik die in Szenario 3.2[109] vorgesehenen Maßnahmen nicht aus, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Auf dieser Grundlage wäre die Verarbeitung nach Szenario 3.2 mit Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO nicht vereinbar, wenn sich ein Verantwortlicher auf diese Maßnahmen beschränken würde.

87. Darüber hinaus könnten die Daten nach Szenario 3.2[110] für einen erheblichen Zeitraum gespeichert werden (d. h. möglicherweise so lange, wie die betroffene Person über ein Konto bei der Fluggesellschaft verfügt). Eine solche Speicherfrist birgt ein höheres Risiko einer Verletzung der Vertraulichkeit und Integrität der Daten und geht offenbar über das für die Zwecke der Verarbeitung unbedingt erforderliche und verhältnismäßige Maß hinaus. Der Ausschuss stellt fest, dass die Datenspeicherfrist für sich genommen kein entscheidender Faktor für die Kompatibilität der besagten Architektur insgesamt mit der DSGVO ist, da sie von den Verantwortlichen geändert werden kann. Auf der Grundlage der dem Ausschuss vorliegenden und in der Beschreibung von Szenario 3.2 enthaltenen Informationen gibt es jedoch keine hinreichende Begründung für diese lange Speicherfrist und keine offensichtlichen Maßnahmen zur Minderung der Risiken für Einzelpersonen. Davon ausgehend wäre die vorgeschlagene Speicherfrist gemäß dem Grundsatz der Speicherbegrenzung in Artikel 5 Absatz 1 Buchstabe e DSGVO nicht auf das notwendige Maß beschränkt.

88. In jedem Fall können die in Szenario 3.2 vorgeschlagenen Maßnahmen die Anforderungen des Artikels 25 DSGVO im Hinblick auf den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nicht erfüllen. In Szenario 3.2 werden die registrierten biometrischen Templates der Fluggäste unter der Kontrolle der Fluggesellschaft oder ihres Cloud-Diensteanbieters (Auftragsverarbeiter) in der Cloud gespeichert. Wie dargelegt, könnten möglicherweise mehrere Einrichtungen Zugang zu diesen Daten haben. Darüber hinaus werden die biometrischen Daten der Fluggäste zur Identifizierung der Fluggäste (1:N-Abgleich) verwendet, wobei N potenziell einem Wert bis zur Gesamtzahl der Kunden der Fluggesellschaft entsprechen kann. Diese Methode hat zur Folge, dass in der zentralen Datenbank eine Person aus einer Gruppe von

[107] Rn. 68 bis 77.
[108] EDSA 2022, Coordinated Enforcement Action on the use of cloud-based services by the public sector, 17. Januar 2023, S. 19.
[109] Siehe Rn. 79–83.
[110] Siehe Rn. 83.

Einzelpersonen gefunden wird, indem jedes erfasste Gesicht verarbeitet wird, um zu überprüfen, ob es mit einer dem System bekannten Person übereinstimmt. Im Gegensatz zu Szenario 3.1 könnte der Vergleich in Szenario 3.2 in einem weitaus größeren Maßstab durchgeführt werden, da das Kriterium hier die Gesamtzahl der Kunden der Fluggesellschaft ist, während Szenario 3.1 nur die Zahl der Fluggäste umfasst, die in einem Zeitraum von mehreren Tagen erwartet werden.

89. Mit Blick auf die Vereinbarkeit mit Artikel 25 DSGVO und insbesondere auf die Erfüllung der Anforderung der Datenminimierung kann die in Szenario 3.2 vorgesehene Verarbeitung darüber hinaus nicht dem Grundsatz der Notwendigkeit entsprechen. Der Ausschuss ist der Auffassung, dass zur Straffung des Fluggaststroms auf Flughäfen ein ähnliches Ergebnis durch andere, weniger einschneidende Maßnahmen erreicht werden könnte, z. B. ohne die Verwendung biometrischer Daten, auch wenn die Nutzererfahrung dann anders wäre, da es möglicherweise länger dauern könnte, das Ausweisdokument und die Bordkarte vorzuzeigen. Darüber hinaus ermöglichen andere Lösungen dem Verantwortlichen, die Ziele in einer weniger in die Privatsphäre eingreifenden Weise zu erreichen, insbesondere solche, die sich auf die Speicherung der biometrischen Daten in einer lokalen Brieftasche auf dem Gerät der betreffenden Einzelperson stützen, oder solche, die eine Verschlüsselung der Daten mit einem bestimmten Schlüssel erfordern, der auf dem Gerät der Einzelperson gespeichert ist.

90. Was den Grundsatz der Verhältnismäßigkeit betrifft, so würde die in Szenario 3.2 vorgesehene Verarbeitung Risiken für die Rechte der betroffenen Personen mit sich bringen, die durch die vorgesehenen Garantien nicht gemindert würden. Die negativen Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen, die sich aus einer Verletzung des Schutzes personenbezogener Daten in einer zentralen Datenbank biometrischer Daten einer großen Zahl von Einzelpersonen, die in der Cloud gespeichert sind, ergeben würden, scheinen den erwarteten Nutzen der Verarbeitung zu überwiegen, da dieser Nutzen, d. h. eine leichte Erhöhung des Komforts und der Geschwindigkeit der Kontrollen, relativ gering ist. Daher kann er die hohe Intensität des Eingriffs dieser Maßnahmen in die Grundrechte und Grundfreiheiten der Einzelpersonen nicht rechtfertigen, sodass die in Szenario 3.2 vorgesehene Verarbeitung nicht als verhältnismäßig angesehen werden kann.

91. In Anbetracht dieser Erwägungen kommt der Ausschuss in Beantwortung der Frage 2.3.1 zu dem Schluss, dass, wenn die Verarbeitung speziell zum Zweck der Straffung des Fluggaststroms auf Flughäfen erfolgt, die in Szenario 3.2 vorgesehene Verarbeitung

- **nicht mit Artikel 25 DSGVO vereinbar sein kann**;
- **Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO nicht entsprechen würde**, wenn sich ein Verantwortlicher auf die in Szenario 3.2 beschriebenen Maßnahmen beschränken würde;
- **Artikel 5 Absatz 1 Buchstabe e DSGVO nicht entsprechen würde**, da die in Szenario 3.2 vorgesehene Aufbewahrungsfrist ausgehend von den Informationen, die dem Ausschuss vorliegen, nicht ausreichend gerechtfertigt ist. Um dem Grundsatz der Speicherbegrenzung in Artikel 5 Absatz 1 Buchstabe e DSGVO nachzukommen, müsste der Verantwortliche nachweisen, dass personenbezogene Daten nicht länger gespeichert werden, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

4 SCHLUSSFOLGERUNGEN

92. Was Frage 1.1 betrifft, kommt der Ausschuss auf der Grundlage des Antrags der französischen Aufsichtsbehörde um Stellungnahme zu den Anforderungen von Artikel 5 Absatz 1 Buchstabe f, Artikel 25 und Artikel 32 DSGVO und auf der Grundlage der vorstehenden Analyse zu dem Schluss, dass

93. der Einsatz von Gesichtserkennungstechnologie zur biometriegestützten Authentifizierung für den spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen (Sicherheitskontrollen, Gepäckaufgabe, Boarding und Zugang zur Fluggastlounge) im Falle einer Speicherarchitektur, bei der das registrierte biometrische Template jedes Fluggastes lokal auf seinem individuellen Gerät und unter seiner alleinigen Kontrolle gespeichert wird, vorbehaltlich geeigneter Garantien gemäß Rn. 46 als grundsätzlich mit den Grundsätzen der Integrität und Vertraulichkeit gemäß Artikel 5 Absatz 1 Buchstabe f sowie Artikel 25 und 32 DSGVO vereinbar angesehen werden könnte.

94. Was Frage 2.1.1 betrifft, kommt der Ausschuss auf der Grundlage des Antrags der französischen Aufsichtsbehörde um Stellungnahme zu den Anforderungen von Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und Artikel 32 DSGVO und auf der Grundlage der vorstehenden Analyse zu dem Schluss, dass

95. der Einsatz von Gesichtserkennungstechnologie zur biometriegestützten Authentifizierung für den spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen (Sicherheitskontrollen, Gepäckaufgabe, Boarding und Zugang zur Fluggastlounge) im Falle einer zentralen Speicherarchitektur, bei der das registrierte biometrische Template jedes Fluggastes in einer zentralen Datenbank in den Einrichtungen des Flughafens unter der Kontrolle des Flughafenbetreibers in verschlüsselter Form mit einem Schlüssel/Passwort im ausschließlichen Zugriff der Einzelperson gespeichert wird, vorbehaltlich geeigneter Garantien gemäß Rn. 60 als grundsätzlich mit dem Grundsatz der Speicherbegrenzung gemäß Artikel 5 Absatz 1 Buchstabe e und mit den Grundsätzen der Integrität und Vertraulichkeit gemäß Artikel 5 Absatz 1 Buchstabe f sowie Artikel 25 und 32 DSGVO vereinbar angesehen werden könnte.

96. Was Frage 2.2.1 betrifft, kommt der Ausschuss auf der Grundlage des Antrags der französischen Aufsichtsbehörde um Stellungnahme zu den Anforderungen von Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und Artikel 32 DSGVO und auf der Grundlage der vorstehenden Analyse zu dem Schluss, dass

97. der Einsatz von Gesichtserkennungstechnologie zur biometriegestützten Identifizierung für den spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen (Sicherheitskontrollen, Gepäckaufgabe, Boarding und Zugang zur Fluggastlounge) im Falle einer zentralen Speicherarchitektur, bei der die registrierten biometrischen Templates der Fluggäste nicht mit einem Schlüssel/Passwort im ausschließlichen Zugriff der einzelnen Fluggäste verschlüsselt und die Templates in einer Datenbank in den Einrichtungen des Flughafens (unter der Kontrolle des Flughafenbetreibers) gespeichert werden, nicht mit Artikel 25 DSGVO vereinbar sein kann. Außerdem würde eine solche Verarbeitung nicht dem Grundsatz der Integrität und Vertraulichkeit gemäß Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO entsprechen, wenn sich ein Verantwortlicher auf die in Szenario 3.1 beschriebenen Maßnahmen beschränken würde.

98. Was Frage 2.3.1 betrifft, kommt der Ausschuss auf der Grundlage des Antrags der französischen Aufsichtsbehörde um Stellungnahme zu den Anforderungen von Artikel 5 Absatz 1 Buchstaben e

und f, Artikel 25 und Artikel 32 DSGVO und auf der Grundlage der vorstehenden Analyse zu dem Schluss, dass

99. der Einsatz von Gesichtserkennungstechnologie zur biometriegestützten Identifizierung für den spezifischen Zweck der Straffung des Fluggaststroms auf Flughäfen (Sicherheitskontrollen, Gepäckaufgabe, Boarding und Zugang zur Fluggastlounge) im Falle einer zentralen Speicherarchitektur, bei der die registrierten biometrischen Templates der Fluggäste nicht mit einem Schlüssel/Passwort im ausschließlichen Zugriff der einzelnen Fluggäste verschlüsselt und die Templates in der Cloud (unter der Kontrolle des Flughafenbetreibers) gespeichert werden, nicht mit Artikel 25 DSGVO vereinbar sein kann. Außerdem würde eine solche Verarbeitung nicht dem Grundsatz der Integrität und Vertraulichkeit gemäß Artikel 5 Absatz 1 Buchstabe f und Artikel 32 DSGVO entsprechen, wenn sich ein Verantwortlicher auf die in Szenario 3.2 beschriebenen Maßnahmen beschränken würde. Schließlich würde, ausgehend von der Beschreibung von Szenario 3.2 und den Informationen, die dem Ausschuss vorliegen, die Verarbeitung nicht dem Grundsatz der Speicherbegrenzung gemäß Artikel 5 Absatz 1 Buchstabe e DSGVO entsprechen.

Für den Europäischen Datenschutzausschuss

Der Vorsitz

(Anu Talus)