Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR

Version 1.1

Adopted on 23 May 2024

Version 1.1	28 May 2024	Grammatical correction in the Executive summary (pages 3 and 4) and paragraphs 77 and 90 of the Opinion
Version 1.0	23 May 2024	Adoption of the Opinion

Executive summary

The French Supervisory Authority requested the European Data Protection Board to issue an opinion on the use of facial recognition technology by airport operators and airline companies for biometric-enabled authentication or identification of passengers to streamline the passenger flow at airports.

As a preliminary remark, the Board recalls that the use of biometric data and in particular facial recognition technology entails heightened risks to data subjects' rights and freedoms. It concerns processing of biometric data which is granted special protection under Article 9 GDPR. Before using such technologies, even if they were to be considered particularly effective, controllers should assess the impact on data subjects' fundamental rights and freedoms and consider whether less intrusive means may achieve their legitimate purpose of the processing.

The scope of this Opinion, as per the request, is limited to the compatibility of the processing with **Article 5(1)(e) and (f), and Articles 25 and 32 GPDR** for the **specific purpose of streamlining the passenger flow at airports** at four specific checkpoints, namely at security checkpoints, baggage drop-off, boarding and access to passenger lounge. This Opinion does not include a full and complete analysis on the compliance with the GDPR by the relevant controller(s) in each case, as well as their processor(s), if applicable. Therefore, this Opinion is without prejudice to a case-by-case legal and technical analysis based on a controller's specific envisaged processing and circumstances. Moreover, the analysis of the applicable legal basis is not within the scope of the questions submitted to the Board in the request and as a result, the validity of consent for such processing, in accordance with Articles 6, 7 and 9 GDPR, is not examined in this Opinion. Furthermore, the present Opinion is without prejudice to the restrictions on the use of biometric data laid down under Member State law.

In this Opinion, the Board assesses the compliance of the processing with the above mentioned GDPR provisions in the context of **four specific scenarios**.

The **first scenario** involves the storage of an enrolled biometric template in the hands of the individual, for example, on their individual device, under their sole control in order to authenticate (1:1 comparison) the passenger as they proceed through the above mentioned airport checkpoints.

The Board concludes that the measures chosen could be considered to have met the necessity principle if the controller can demonstrate that there are no less intrusive alternative solutions that could achieve the same objective as effectively. In addition, the intrusiveness of the processing can be counterbalanced by the active involvement of the passengers as their biometric template is stored in their hands only, for example, on their individual device, under their sole control and their data is deleted shortly after the matching is completed. On this basis, the Board concludes that the processing envisaged in the first scenario **could be considered in principle compatible with Articles 5(1)(f), 25 and 32 GDPR** subject to the implementation of appropriate safeguards.

The Board has identified safeguards which as a minimum should be implemented for a solution similar to the first scenario.

The **second scenario** involves the centralised storage, within the airport, of an enrolled biometric template in an encrypted form with a key/ secret solely in the passenger's hands. This enables passenger authentication (1:1 comparison) as they proceed through the above mentioned airport checkpoints. The enrolment is valid for a given period, which, for example, could be up to one year after the last flight was taken up to the passport expiry date.

The Board concludes that the processing could be considered to have met the necessity principle if the controller can demonstrate that there are no less intrusive alternative solutions that could achieve the same objective as effectively. Moreover, the intrusiveness of the processing can be counterbalanced by the active involvement of the passenger as they hold under their sole control the key/ secret to their encrypted biometric data. Assuming the controller implements appropriate safeguards, security risks from using a centralised database in this scenario could be mitigated and the negative impact on the data subjects' fundamental rights and freedoms could be considered proportional to the anticipated benefit. Regarding the principle of storage limitation, no information has been provided to the Board to substantiate the long storage period. In order to achieve compatibility with Article 5(1)(e) GDPR in this scenario, the controllers should be able to justify why the envisaged retention period is necessary for the purpose in specific cases. The Board recommends that controllers envisage the shortest possible storage period while offering passengers the option to set their preferred storage period. On this basis, the Board concludes that the processing envisaged in scenario 2 **could be considered in principle compatible with Articles 5(1)(e), 5(1)(f), 25 and 32 GDPR,** subject to the implementation of appropriate safeguards.

The Board has identified safeguards which as a minimum should be implemented for a solution similar to the second scenario.

The **third scenario** involves the centralised storage of an enrolled biometric template in an encrypted form within the airport under the airport operator's control. This enables passenger identification (1:N comparison), as they proceed through the above mentioned airport checkpoints. The storage period in this scenario is typically 48 hours and the data is deleted once the plane has taken off.

As the storage of the ID and biometric data is in a central database, if the confidentiality of the database is compromised, it may subsequently entail access to the whole set of data and could enable unauthorised or unlawful identification of passengers in other environments. The centralised storage architecture under the control of the airport operator also leads to the passenger losing control of their data to a greater extent. The Board considers that a similar result to streamlining the passenger flow at airports can be achieved in a less intrusive manner and the negative impact on the data subjects' fundamental rights and freedoms that would result from a data breach in a centralised database of biometric data seems to outweigh the anticipated benefit resulting from the processing. Therefore, the processing cannot meet the necessity and proportionality principles. On this basis, the Board concludes that the processing envisaged in the third scenario **cannot be compatible with Article 25 GDPR**. Also, it **would not comply with Articles 5(1)(f) and 32 GDPR** if a controller would limit themselves to the measures as described in this scenario.

The **fourth scenario** involves the centralised storage of an enrolled biometric template in an encrypted form in the cloud under the control of the airline company or its cloud service provider. This enables passenger identification (1:N comparison) as they proceed through the above mentioned airport checkpoints. The storage period in this scenario can potentially be for as long as the customer holds an account with the airline company.

As the storage of the ID and biometric data is in a central database in the cloud, multiple entities could have access to such data, including possibly non-EEA providers. The passenger's data is decrypted when in use and the keys are under the control of the airline company or its processors, which could increase the security exposure surface. Such centralised storage architecture also leads to the passenger losing control of their data to a greater extent. The data could also be stored for a significant period of time, which exposes the data to higher risks of a security breach and seems to go beyond

what is strictly necessary and proportionate for the purposes of processing, unless further apparent measures are taken to mitigate the risks to individuals.

The Board considers that a similar result to streamlining the passenger flow at airports can be achieved in a less intrusive manner and the negative impact on the data subjects' fundamental rights and freedoms that could result from a data breach in a centralised database of biometric data seems to outweigh the anticipated benefit resulting from the processing. Therefore, the processing cannot meet the necessity and proportionality principles. On this basis, the Board concludes that the processing envisaged in the fourth scenario **cannot be compatible with Article 25 GDPR**. Also, it **would not comply with Article 5(1)(e) GDPR** based on the information available to the Board and **would not comply with Articles 5(1)(f) and 32 GDPR** if a controller would limit themselves to the measures as described in this scenario.

Table of contents

1 INTRODUCTION 6
1.1 Summary of facts 6
1.2 Admissibility of the request for an Article 64(2) GDPR Opinion 8
2 SCOPE AND CONTEXT OF THE OPINION 9
2.1 Scope of the Opinion 9
2.2 Key notions 12
3 On the merits of the request 14
3.1 General observations 14
3.2 On compatibility with Article 5(1)(e) and (f), Articles 25 and 32 GDPR 16
3.2.1 Scenario 1: storage of enrolled biometric template only in the hands of the individual, for authentication 16
3.2.2 Scenario 2: centralised storage of enrolled biometric template in an encrypted form within the airport and with a key/ secret solely in the passengers' hands, for authentication ..24
3.2.3 Centralised storage of the enrolled biometric templates for identification 28
3.2.3.1 Scenario 3.1: centralised storage in a database within the airport, under the control of the airport operator 28
3.2.3.2 Scenario 3.2: centralised storage in a cloud, under the control of the airline company 32
4 CONCLUSIONS 34

The European Data Protection Board

Having regard to Article 63 and Article 64(2) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "**GDPR**"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 10 and Article 22 of the European Data Protection Board's (hereinafter the "**Board**" or the "**EDPB**") Rules of Procedure (hereinafter "**EDPB RoP**"),

Whereas:

(1) The main role of the Board is to ensure the consistent application of the GDPR throughout the European Economic Area (hereinafter "**EEA**"). Article 64(2) GDPR provides that any supervisory authority (hereinafter "**SA**"), the Chair of the Board or the European Commission may request that any matter of general application or producing effects in more than one EEA Member State be examined by the Board with a view to obtaining an opinion.

(2) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB RoP within eight weeks from when the Chair and the competent SA have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

has adopted the following opinion:

1 INTRODUCTION

1.1 Summary of facts

1. On 16 February 2024, the French Supervisory Authority (hereinafter the "**FR SA**") requested the Board to issue an opinion on the compatibility with Article 5(1)(e) and (f), and Articles 25 and 32 GDPR of the use of facial recognition technology by airport operators and airline companies for biometric-enabled authentication or identification of passengers[2], in order to streamline the passenger flow, at airport security checkpoints[3], baggage drop-off, boarding, and access to passenger lounge (excluding border control and checks carried out by duty-free shops) (hereinafter the "**Request**"). The FR SA attached to its Request a description of typical use cases (Annex I).

[1] References to "**Member States**" made throughout this opinion should be understood as references to "EEA Member States". References to the "Union" or "EU" made throughout this opinion should be understood as references to the "EEA".

[2] In the context of this Opinion "**passenger**" means a data subject, whose personal data are processed for the specific purpose described in this Opinion. Hereinafter in this Opinion, the terms "passenger" and "individual" are used interchangeably.

[3] For the purposes of this Opinion, "**airport security checkpoints**" refers to the security checks performed under the responsibility of the airport operator that passengers need to undergo, in order to enter from the departures' hall to the boarding area or boarding gate.

2. In its Request, the FR SA observes that the models that are currently being tested in several EU airports vary from one Member State to the other, thus possibly creating a risk of divergence between the interpretations among SAs and a risk that different effects would be produced for the fundamental rights and freedoms of data subjects in the EU[4].

3. The Board considers that, in order to provide a reply to the Request, the following questions need to be answered:

4. **Question 1**:

1.1. Can the use of facial recognition technology for biometrics-enabled authentication **for the specific purpose of streamlining the passenger flow at airports** (security checkpoints, baggage drop-off, boarding and access to passenger lounge) be compatible with **Article 5(1)(f), Articles 25 and 32 GDPR,** in the case of a storage architecture, where the biometric template of each passenger is stored **only in the hands of the individual**, e.g. locally on their individual device, under their sole control?

1.2. If such processing would be found compatible with the above-mentioned provisions, what minimum appropriate safeguards would be needed, in light of Articles 25 and 32 GDPR?

Question 2:

2.1. Can the use of facial recognition technology for biometrics-enabled authentication or identification **for the specific purpose of streamlining the passenger flow at airports** (security checkpoints, baggage drop-off, boarding and access to passenger lounge) be compatible with **Article 5(1)(e) and (f), and Articles 25 and 32 GDPR** in the case of a **centralised** storage architecture, where the biometric template of each passenger is stored in a central database:

2.1.1. In a central database within the airport, under the control of the airport operator, in an encrypted form, with a key/ secret held solely in the hands of the individual (for instance in the individual's mobile phone), for authentication?

2.1.2. If such processing would be found compatible, what minimum appropriate safeguards would be needed, in light of Articles 25 and 32 GDPR?

2.2.1. In a central database within the airport, under the control of the airport operator, in an encrypted form, with keys held by the airport operator, for identification?

2.2.2. If such processing would be found compatible, what minimum appropriate safeguards would be needed, in light of Articles 25 and 32 GDPR?

2.3.1. In the cloud, under the control of the airline company or its service provider (processor), in an encrypted form, with keys held by the airline company or its service provider, for identification?

[4] Request, p. 1.

2.3.2. If such processing would be found compatible, what minimum appropriate safeguards would be needed, in light of Articles 25 and 32 GDPR?

5. After the FR SA considered the file to be complete on 16 February 2024 and the Chair of the Board considered the file to be complete on 23 February 2024, the file was circulated by the Secretariat on 23 February 2024. The Chair of the Board decided, in compliance with Article 64(3) GDPR in conjunction with Article 10(2) EDPB RoP, to extend the default timeline of eight weeks by a further six weeks on account of the complexity of the subject-matter.

1.2 Admissibility of the request for an Article 64(2) GDPR Opinion

6. Article 64(2) GDPR provides that, in particular, any SA may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion.

7. The Board considers that the request referred by the FR SA on the compatibility of the use of facial recognition technology for biometrics enabled authentication or identification for the specific purpose of streamlining the passenger flow at airports relates to questions "producing effects in more than one Member State", because, as explained in the Request[5], there are currently several projects under deployment in the Member States' airports, and it is estimated that such use will increase in the coming years. The models that are currently being tested by different airports and airlines vary significantly from one Member State to the other, thus possibly creating a risk that, from a data protection perspective, diverging effects would be produced in more than one Member State.

8. Also, the Board considers that the Request referred by the FR SA has important consequences for the application of the principles set out under Article 5(1)(e) and (f) GDPR, and the requirements applicable to controllers under Article 25 GDPR, as well as the requirements applicable to controllers and processors under Article 32 GDPR. Therefore, this request concerns a "matter of general application" within the meaning of Article 64(2) GDPR, as it relates to the consistent interpretation of the principles of storage limitation (Article 5(1)(e) GDPR) and integrity and confidentiality (Article 5(1)(f) GDPR), and the notions of data protection by design and by default (Article 25 GDPR) and data security (Article 32 GDPR) to ensure, amongst others, the consistent application of those provisions in the EEA.

9. Any possible divergent positions across Member States on the interpretation of Article 5(1)(e) and (f), and Articles 25 and 32 GDPR would amplify the risk that airport operators and airline companies develop facial recognition projects in a non-consistent manner. As the FR SA has demonstrated the clear need for a consistent interpretation of these provisions in relation to the facial recognition technology for biometric-enabled authentication or identification of passengers, in order to streamline the passenger flow at airports[6], the Board considers that the Request is reasoned, in line with Article 10(3) of the EDPB RoP.

10. According to Article 64(3) GDPR, the EDPB shall not issue an opinion if it has already issued an opinion on the matter[7]. The EDPB has not yet provided replies to the questions arising from the Request.

[5] Request, p. 3.
[6] Request, p. 1-3.
[7] Article 64(3) GDPR and Article 10(4) of the EDPB Rules of Procedure.

Although EDPB Guidelines 3/2019 on video devices[8] already provide some useful elements on the security measures that should be applied to the processing of biometric data, they do not address all the aspects regarding the questions raised in the Request. Further, the available EDPB guidance, including EDPB Guidelines 3/2019 on video devices, do not provide specific guidance on possible elements to be verified in relation to centralised or decentralised storage of biometric data for identifying or authenticating passengers to streamline the passenger flow at airports, and on the compatibility of such processing with Article 5(1)(e) and (f), and Articles 25 and 32 GDPR.

11. For these reasons, the Board considers that the Request is admissible and the questions it raised should be analysed in an opinion adopted pursuant to Article 64(2) GDPR.

2 SCOPE AND CONTEXT OF THE OPINION

2.1 Scope of the Opinion

12. This Opinion concerns only the compatibility with Article 5(1)(e) and (f), and Articles 25 and 32 GPDR of the use of facial recognition technology for the biometrics-enabled authentication or identification of passengers by airport operators and airline companies, **for the specific purpose of streamlining the passenger flow at airports**, namely at security checkpoints, baggage drop-off, boarding and access to passenger lounge, as per the Request.

13. Regarding the **scope of this Opinion**, the Board clarifies the following:

1) Processing of personal data in the framework of border controls and checks carried out by duty-free shops do not fall in the scope of this Opinion, as they are carried out by controllers other than airport operators and airline companies.

2) The use of facial recognition technology, even if based on the scenarios described below in section 3.2, for any other purposes (such as law enforcement) or by any other parties, even if for similar purposes, is outside the scope of this Opinion.

3) This Opinion only examines the processing of personal data of passengers and it does not cover other types of data subjects, such as airport operators' or airline companies' staff.

4) This Opinion examines the Request as submitted by the FR SA, in relation to the compatibility of the storage architectures of the passengers' biometric templates with Article 5(1)(e) and (f), and Articles 25 and 32 GDPR. In this regard, this Opinion does not include a full and complete analysis on the compliance with the GDPR, by the relevant controller(s) in each case, as well as their processor(s), if applicable. This is particularly important considering that these technologies entail heightened risks associated with the processing of the special categories of data in accordance with Article 9 GDPR. Therefore, this Opinion is without prejudice to an assessment regarding other GDPR provisions when it comes to the use of facial recognition technologies, including in the specific sector addressed by the Request, or to case-by-

[8] EDPB Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020 (hereinafter "**EDPB Guidelines 3/2019 on video devices**").

case legal and technical analysis based on a controller's specific envisaged processing and circumstances.

5) This Opinion does not examine the processing of children's personal data and is without prejudice to any specific requirements that apply in that respect.

6) This Opinion is without prejudice to legal requirements and further restrictions on the use of biometric data stemming from national laws of Member States[9].

7) Any conclusion in this Opinion is without prejudice to further technological developments.

8) This Opinion examines four scenarios, whose specific characteristics are described below in section 3.2. It does not address other scenarios even if the processing is done for the same purposes.

14. In its Request, the FR SA indicated that the processing of passengers' biometric data for the purpose of streamlining the passenger flow at airports would be based on the assumption that the individuals consent to such processing, which would possibly form the legal basis under GDPR[10]. **However, the analysis of the applicable legal basis is not within the scope of the questions submitted to the EDPB in the Request and thus, the validity of consent for such processing in accordance with Articles 6, 7 and 9 GDPR is not examined in this Opinion.**

15. Nevertheless, the EDPB notes in general terms that, if the relevant controllers were to rely on this legal basis, they would need to obtain a valid explicit consent[11] from the individuals willing to use such services. Such explicit consent would need to be freely given, specific and informed[12] and whether those conditions are met would be analysed on a case by case basis. This, *inter alia*, means that:

1) Individuals would need to be able to easily withdraw such consent at any time and without any detriment[13].

2) In order for consent to be freely given, such use of biometric-enabled technologies can only take place on a voluntary basis, as individuals should be able to freely choose whether or not to use these services and without any detriment (such as significantly

[9] For example, Article 9(4) GDPR provides that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of biometric data.
[10] Request, Annex I.
[11] According to Articles 4(14) and 9(1) GDPR, as well as Article 9(2)(a) GDPR, the processing of biometric data for the purpose of uniquely identifying a natural person shall be prohibited, unless the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in Article 9(1) GDPR may not be lifted by the data subject. See also Recitals 51, 52, and 53 GDPR.
[12] Articles 4(11) and 7 GDPR.
[13] Article 7(4) GDPR, also Recital 50 GDPR.

longer delays for passengers who do not consent[14]), incentives, additional costs or additional advantages in return[15].

3) Explicit consent would also need to be sought from individuals whose biometric data are processed, even if they have not enrolled to be identified or authenticated by such means. In other words, it is essential that individuals who did not explicitly consent to facial recognition for the purpose intended would not have their faces scanned by cameras. This can be achieved, for instance, by dedicating specific lanes to facial recognition and providing appropriate signage and physical separation with the non-biometric control flows to allow a clear identification of such lanes.

4) Without prejudice to whether consent would be the applicable legal basis for such processing, the principles of processing enshrined in Article 5 GDPR with regard to necessity and proportionality, still apply even when individuals have provided their explicit consent to the use of their biometric data[16].

16. The Request specifies[17] that airport operators would act as controllers regarding the processing at airport security checkpoints, while airline companies would act as controllers regarding the processing at baggage drop-off, boarding and access to passenger lounge. Therefore, the Board notes that different actors might be involved in the processing described in the Request and it has not assessed the application of the roles of (joint) controller and/ processor in the scenarios described below in section 3.2 of this Opinion. In each case the actors involved need to be identified and their responsibilities clearly allocated, so the requirements of the GDPR are met[18].

17. Additionally, the Board notes that currently there is no uniform legal requirement in the EU for airport operators and airline companies to identify passengers and to verify that the name on the passenger's boarding card matches the name on their identity document in all above mentioned checkpoints[19]. Thus, any such requirements are subject to national laws that may vary from one Member State to another. In some Member States, such verification may be required for some checkpoints (e.g.

[14] For instance, this might include considerations such as designing a system to avoid creating social pressure on passengers who do not want to consent, by avoiding that its choice would impact negatively on other passengers.
[15] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020 (hereinafter "**EDPB Guidelines 5/2020 on consent**"), paragraphs 46, 48.
[16] Idem, paragraph 5.
[17] Request, Annex I.
[18] In line with Articles 4(7) and (8), 5(2), 24, 26, 28 and 29 GDPR. See also EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021.
[19] The relevant regulation at EU level is Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security. However, this regulation does not address checks of official identity documents at checkpoints at airports, and Member States have discretion to regulate this at national level.

baggage drop-off or boarding), while in others no such checks are required today[20]. The existence of legal duties to verify passengers' identity has a direct impact on the different airports' practices.

18. Consequently, in these situations, **where no verification of the passengers' identity with an official identity document is required, no verification with the use of biometric should be performed, as this would result in an excessive processing of data since it entails the processing of additional data compared to the current situation and would go beyond what is necessary for the relevant purpose, in breach of the data minimisation principle set out by Article 5(1)(c) GDPR.** Such consideration should be borne in mind in relation to the examination of all scenarios described below in section 3.2 of this Opinion.

2.2 Key notions

19. To qualify as biometric data under Article 4(14) GDPR[21], processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, should imply a measurement of these characteristics, since biometric data is the result of such measurements[22].

20. By using the image of an individual's face (a photograph or video) called a biometric "**sample**", it is possible to extract a digital representation of distinct characteristics of such face (this is called a "**template**")[23]. In addition, the Board recalls that "[a] biometric template is a digital representation of the unique features that have been extracted from a biometric sample and can be stored in a biometric database"[24] which allow or confirm the unique identification of a natural person. Furthermore, "[t]his biometric template is supposed to be unique and specific to each individual and it is, in principle, permanent over time"[25]. Typically, in a comparison process aiming at identifying or authenticating an individual via facial recognition, an incoming biometric template is compared against objects stored to either verify a match or find one in a database[26].

[20] Meaning that currently either no verification is performed at all or only the existence of the boarding pass is verified. For example, based on Protocol concerning the exemption of nationals of Denmark, Finland, Norway and Sweden from the obligation to have a passport or residence permit while resident in a Scandinavian country other than their own of 22 May 1954, as of 1 July 1954, citizens of Norway, Denmark, Finland and Sweden are exempted from the obligation to hold a passport or other travel identification when traveling between these countries.

[21] See also Recitals 51, 52 and 53 GDPR.

[22] EDPB Guidelines 3/2019 on video devices, paragraph 74.

[23] EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, adopted on 26 April 2023 (hereinafter "**EDPB Guidelines 5/2022 on facial recognition in law enforcement**"), paragraphs 7 and 8.

[24] Idem, paragraph 9.

[25] Idem.

[26] EDPB Guidelines 5/2022 on facial recognition in law enforcement, paragraphs 10-11; see also International standard ISO/IEC 2382-37, 2022-03, available at: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [last accessed on 23 May 2024] (hereinafter "**ISO/IEC 2382-37**")

21. Facial recognition technology can fulfil two distinct functions – authentication[27] and identification[28]. While both functions are distinct, they both rely on the processing of biometric data related to an identified or identifiable natural person[29] and, therefore, constitute processing of special categories of personal data under Article 9 GDPR[30].

22. In particular:

> **Authentication** aims at confirming a biometric claim through comparison. This is also called 1-to-1 verification.
>
> **Identification** aims at searching against a biometric enrolment database to return identifiers attributable to a single individual. This is also called 1-to-many identification.

23. In both cases (i.e. identification and authentication), the facial recognition techniques are based on an estimated match between templates; i.e. the one being compared and the baseline(s). From this point of view, they are probabilistic: the comparison deduces a higher or lower probability that the person is indeed the person to be authenticated or identified; if this probability exceeds a certain threshold in the system, defined by the user or the developer of the system, the system will assume that there is a match to be identified or authenticated[31].

[27] The Board notes that the forthcoming Regulation of the European Parliament and of the Council laying down the harmonised rules on artificial intelligence (Artificial Intelligence Act) (not yet published in the Official Journal), also defines in Article 3(36) "biometric verification" as "the automated, one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data" (see European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[28] Idem, Article 3(35) of the Artificial Intelligence Act defines "biometric identification" as "the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database".

[29] ISO/IEC 2382-37.

[30] Article 4(14) GDPR and EDPB Guidelines 5/2022 on facial recognition in law enforcement, paragraph 12.

[31] EDPB Guidelines 5/2022 on facial recognition in law enforcement, paragraph 11. See also ISO/IEC 2382-37.

3 ON THE MERITS OF THE REQUEST

3.1 General observations

24. This section analyses the questions presented in paragraph 4 above. In this context, the Board will analyse, for question 1, compatibility with Article 5(1)(f), and Articles 25 and 32 GDPR, and for question 2, compatibility with Article 5(1)(e) and (f), and Articles 25 and 32 GDPR.

25. For this purpose, the Board will analyse four different scenarios[32], whose specific characteristics are described below in section 3.2.

26. As a preliminary remark, the Board recalls that the use of biometric data and in particular facial recognition technology entails heightened risks to data subjects' rights and freedoms. In the first place, the processing at stake concerns biometric data which is granted special protection under Article 9 GDPR. Notably, biometric data changes irreversibly the relation between body and identity because they make the characteristics of the human body "machine-readable" and subject to further use[33]. Moreover, the use of facial recognition technology can lead to risks associated with false negatives, bias and discrimination,[34] and the potential for misuse of biometric data could have grave consequences to individuals such as identity fraud or impersonation[35]. It should also be noted that, when facial recognition is done remotely and without active involvement of the data subject, individuals might be even less aware about such processing and associated risks. Finally, it is important to emphasise that the characteristics on which biometric data is based can generally be considered as permanent and should be treated as being non-revocable, especially in the context of facial recognition[36].

27. Therefore, taking into account the above, before using such technologies, even if they were to be considered particularly effective, controllers should assess the impact on data subjects' fundamental rights and freedoms and consider whether less intrusive means may achieve their legitimate purpose of the processing[37].

---

[32] The four scenarios analysed by the Board are based on use cases presented in Annex I of the Request. The FR SA has clarified that the use cases presented in Annex I of the Request are examples of implementation, belonging to a scenario, used for illustrative purposes.

[33] Article 29 Working Party Opinion 3/2012 on developments in biometric technologies adopted on 27 April 2012, WP193 (hereinafter "**Article 29 WP Opinion 3/2012 on biometric technologies**"), p. 4. It should be noted that this Opinion refers to Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive"). The GDPR has broadened the scope of the special categories of data and, unlike the Data Protection Directive, the GDPR provides that biometric data are special categories of data (Article 9 GDPR).

[34] Guidelines on facial recognition, Consultative Committee of Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data, June 2021, p. 15; also EDPB Guidelines 5/2022 on facial recognition in law enforcement, paragraph 27.

[35] Article 29 WP Opinion 3/2012 on biometric technologies, p. 29.

[36] EDPB Guidelines 5/2022 on facial recognition in law enforcement, paragraph 104.

[37] Recital 39 GDPR. See also EDPB Guidelines 3/2019 on video devices, paragraph 73.

28. The Board also recalls that the right to the protection of personal data is not an absolute right and should be balanced against other fundamental rights protected by the Charter in accordance with the principle of proportionality[38].

29. Article 25(1) GDPR refers to "the data protection principles" that are listed in Article 5 GDPR[39] and requires to implement them by design "in an effective manner"[40]. This expressly includes the principle of data minimisation under Article 5(1)(c) GDPR,[41] which requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, giving expression to the principle of proportionality"[42]. In addition, Article 25(2) GDPR specifies the "data minimisation by default" obligation, by stating that it applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility[43].

30. However, Article 25 GDPR does not require controllers to implement any specific technical and organisational measures, and rather requires that the chosen measures and safeguards should be specific to the context and risks for the rights and freedoms of the data subject posed by the processing[44]. Similarly, Article 32 GDPR on security of processing requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the rights and freedoms of natural persons.

31. Importantly, even if passengers were to explicitly consent to the use of their biometric data in order to streamline the passenger flow at airports, the principles of processing enshrined in GDPR regarding necessity and proportionality still apply and need to be complied with[45].

---

[38] Recital 4 GDPR. See also in this regard, Judgment of the Court of Justice of 22 June 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504 (hereinafter "C-439/19 *Latvijas Republikas Saeima*"), paragraphs 98, 110 and 113. Moreover, the principle of proportionality, as a general principle of EU law, requires that measures implemented by acts of the Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it (See Judgment of the Court of Justice of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, ECLI:EU:C:2010:662 (hereinafter "C-92/09 and C-93/09 *Volker und Schecke*"), paragraph 74 and the case-law cited).

[39] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020 (hereinafter "**EDPB Guidelines 4/2019 on Data Protection by Design and Default**"), paragraph 11.

[40] Article 25(1) GDPR states that: 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'. See also EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, paragraph 13.

[41] Correspondingly, Recital 39 GDPR states that personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

[42] C-439/19 *Latvijas Republikas Saeima*, paragraph 98; Judgment of the Court of Justice of 11 December 2019, *Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (hereinafter "C-708/18 *M5A-ScaraA*"), paragraph 48.

[43] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, paragraph 48.

[44] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, paragraph 14.

[45] EDBP Guidelines 5/2020 on consent under Regulation 2016/679, paragraph 5.

32. Regarding the **necessity principle**, the Board will consider whether the proposed processing is necessary to meet the objective pursued and whether the same objective can be achieved as effectively by other means less intrusive to the fundamental rights and freedoms of data subject[46]. Regarding the **proportionality principle**, the Board will assess whether the negative impact on the data subjects' fundamental rights and freedoms is proportional to any anticipated benefit. If the benefit is relatively minor, then such impact might not be proportionate[47].

33. In any case, even if the Board considers that one of the scenarios analysed below could meet the requirements of Articles 5(1)(e) and (f), 25 and 32 GDPR, it is up to the controller in each case to demonstrate this with factual elements. Such demonstration should include consideration of alternative scenarios.

3.2 On compatibility with Article 5(1)(e) and (f), Articles 25 and 32 GDPR

3.2.1 Scenario 1: storage of enrolled biometric template only in the hands of the individual, for authentication

34. This section examines the compatibility with Article 5(1)(f), and Articles 25 and 32 GDPR of storage of passengers' biometric template only in the hands of the individual, for example on their individual device[48], under their sole control[49], for authentication[50] (hereinafter "**Scenario 1**"). This section also examines the appropriate safeguards for Scenario 1, in light of Articles 25 and 32 GDPR.

Description of the Scenario

35. In Scenario 1, the enrolled biometric template of each passenger, who has consented to such processing, is only stored in the hands of the individual, for example, on an individual device kept by each passenger, under their sole control. The passengers are authenticated (1:1 comparison), when going through specific checkpoints at the airport.

36. Enrolment is done by the airport operator, either remotely through the airport operator's app[51] or at the airport terminals with appropriate identity assurance level (e.g. eIDAS appropriate level of assurance[52]). Such enrolment consists of recording, on the passenger's device, a biometric template and the identification data[53] (hereinafter "**ID**") necessary for the processing. The enrolment occurs

[46] C-439/19 *Latvijas Republikas Saeima*, paragraphs 110 and 113; Judgement of the Court of Justice (Grand Chamber) of 4 July 2023, *Meta v. Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, paragraph 108.
[47] C-708/18 *M5A-ScaraA*, paragraphs 52-56, C-92/09 and C-93/09 *Volker und Schecke*, paragraph 87, C-439/19 *Latvijas Republikas Saeima*, paragraphs 98, 110, 113. See also Article 29 WP Opinion 3/2012 on biometric technologies, p. 8.
[48] As an alternative, the individual could print and store their biometric template on paper.
[49] This is without prejudice to the overall responsibility of the controller regarding the processing.
[50] As exemplified by use case 1 in Annex I of the Request.
[51] The EDPB notes that alternatives ways for such enrolment could be envisaged in the future and the enrolment could possibly be carried without a specific airport operator's app, for example, by means of interaction with a user's digital wallet.
[52] A framework for electronic identification and trust services (hereinafter "**eIDAS**") based on Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
[53] For the purposes of this Opinion, identification data denotes data, such as family name, first name, date of birth, etc., which has been verified as accurate with regards to an identity document or passport.

only once and for a specific validity period (for instance, aligned with the validity period of the passengers' passport). Neither the passengers' ID, nor their biometric data are retained by the airport operator after the enrolment process.

37. In particular regarding storage, the passenger's ID and biometric template are stored locally on each passenger's device (e.g. the airport operator's mobile app or in a digital wallet app). The device then can be used to transmit or query the passengers' ID and biometric template, possibly including flight information and/ or the boarding pass. For instance, this information is encrypted with a key only held by the airport operator— maybe encoded in the form of a QR code, which can be either printed on paper or displayed on the passenger's device screen. In this instance, the passenger would then show this QR code to dedicated control pods at the airport, equipped with a QR scanner and a camera.

38. In terms of security, during matching, QR codes are decrypted with a key held by the airport operator, who is the only one able to decrypt the QR codes. The passengers' biometric data is retained only for a very short period and deleted after the matching is completed. It should be noted that security measures as regards storage partly depend on the passenger's device security.

EDPB's assessment

39. Scenario 1 describes technical and organisational measures that are designed to ensure a level of security appropriate to the risks to data subjects as required under Articles 5(1)(f) and 32 GDPR. The passengers are authenticated (1:1 comparison), when going through specific checkpoints at the airport. In this scenario, the main matching operation is done in the context of a controlled environment[54], where the passengers are actively involved and have more control over their data. In particular, only passengers who consented to such processing would be checked and, as they would be checked at dedicated pods, biometric data of other passengers who did not consent to such processing would not be collected. In addition, the consenting passengers have a possibility to stop the processing at any moment by deleting the data from their device.

40. The use of facial recognition based on a biometric template stored only in the hands of the individual, which may, for example, be on an individual device kept by the passenger, under their sole control, used for authentication at specific checkpoints through a dedicated interface, presents, under certain conditions, less risks compared to the use of biometric data where the data are stored in a centralised database[55]. Such localised storage, when accompanied by appropriate safeguards[56], reduces the severity of personal data breaches in comparison with centralised storage, when it comes to number of individuals affected, and ensures that access to the biometric template involves an active involvement of the data subject.

41. Furthermore, the matching could be done locally at the airport, by comparing the biometric template, for example contained in the QR code, with the output of the template calculated based on the biometric sample captured by the control pod's camera. Only the matching result would be made

[54] "Uncontrolled environment" refers to use of facial recognition for identification without the active involvement of the data subjects, where the template of each face entering the monitoring area is compared with templates from a broad cross-section of the population stored in a database, see EDPB Guidelines 5/2022 on facial recognition in law enforcement, paragraph 17.
[55] EDPB Guidelines 5/2022 on facial recognition in law enforcement, paragraph 17.
[56] As addressed below from paragraph 46.

known to and used by the controller performing a specific check (that could be either an airport operator or an airline company depending on whether it is done at the airport security checkpoints, the baggage drop-off, boarding, and/ or access to passenger lounge). In addition, the fact that the information required for the matching (e.g. the QR code) needs to be given by the individual acts as a second factor[57] and thus reinforces the security of the authentication.

42. Regarding the compatibility with Article 25 GDPR and in particular in order to comply with the requirement of data minimisation, it should be ensured that the processing meets the necessity principle. In Scenario 1 the measures chosen could be considered to have met the necessity principle in relation to the purpose pursued (i.e. streamlining the passengers' flow) if, depending on the circumstances of the processing, the controller can demonstrate that there are no less intrusive alternative solutions that could achieve the same objective as effectively. For example, the controller may be able to demonstrate that, even if the passengers would have to show their device, Scenario 1 speeds up the verification process compared to the current situation which it includes a human checking whether the name on the boarding pass matches the passenger's identity document[58]. Notably, this could not be shown if there are currently no checks performed to verify the passengers' identity based on their official identity document (in this regard, see paragraph 18 above).

43. In addition, biometric templates are not retained by the airport operator after the enrolment and the retention period of the biometric data by the controller performing the check is very short, as such data are deleted as soon as the matching is completed. Thus, the measures chosen in Scenario 1 seem to limit the extent of the processing and the storage period of the personal data.

44. Regarding the proportionality principle, the intrusiveness from such processing can be counterbalanced by the active involvement of the passengers, as their biometric data would be stored in their hands only. In addition, taking into account the measures described above and assuming that the controller implements appropriate safeguards as required by the specific processing in question, the implementation of appropriate measures could ensure a level of security appropriate to the risk. In that case, the negative impact on the data subjects' fundamental rights and freedoms could be considered as proportional to the anticipated benefit.

45. Therefore, taking into account the above, in reply to question 1.1, the Board concludes that such processing **could be considered to be in principle compatible with Articles 5(1)(f), 25 and 32 GDPR, subject to appropriate safeguards**.

Appropriate safeguards

46. In this type of scenario, in reply to question 1.2, the EDPB considers that at least the following safeguards should be implemented. *Other safeguards than the ones described in this Opinion could be used to achieve the same security and data protection goals and could be lawful as long as they ensure compliance with the applicable legal framework*.

47. Note: *this is a high level and non-exhaustive overview of the possible appropriate safeguards, which should be implemented by a controller in a solution similar to Scenario 1. Their appropriateness under Articles 25 and 32 GDPR will depend on a case by case analysis. All controllers will need to ensure that*

[57] For example, this mitigates the risk of identity spoofing. See also safeguard C.1.2 below.
[58] It could also be argued that the biometric check may be less prone to errors than compared to a human check.

*they conduct their own Data Protection Impact Assessment (hereinafter "**DPIA**")[59] and their specific solutions may require additional measures not included in this Opinion.*

A. General

A.1 Data Processing impact assessment

A.1.1 Carry out a DPIA, in line with Article 35 GDPR requirements, whenever the controller plans a new processing operation involving processing likely to result in a high risk. This is likely to be the case with Scenario 1, as it involves processing biometric data on a large scale[60]. Evaluate the appropriateness of implementing a facial recognition system, including its necessity and proportionality in relation to the purposes pursued[61], during the early design phase and review it throughout the lifecycle of the product development;

A.1.2 Consult the relevant supervisory authority should the processing still result in a high risk despite the measures taken by the controller to mitigate the risk[62].

A.2 Data Subject Rights and safeguards that can be implemented by controllers

A.2.1 Safeguards to address cases of a false negative. Mitigate the risk of age, gender and racial bias by "regularly assessing whether algorithms are functioning in line with the purposes and adjusting the algorithms to mitigate uncovered biases and ensure fairness in the processing"[63]. For example, by implementing human oversight and intervention, in order to mitigate any biases and ensure that there is no stigmatisation or profiling of passengers;

A.2.2 Ensure all processing of personal data is transparent and individuals are aware and in control of how their data is processed for each processing operation[64];

A.2.3 Ensure measures are in place to comply with the purpose limitation principle so that the data is not used for other purposes, such as security or training purposes;

A.2.4 Ensure no photo or video is captured, even if not recorded and not processed, from individuals who do not consent to the facial recognition through appropriate measures (such as using an adequate depth of field and capture area to avoid capturing images from other passengers in the background or around, deploying dedicated queues clearly labelled for facial recognition);

[59] Article 35 GDPR.
[60] Article 35(3) GDPR and WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 13 October 2017, WP248rev.01, endorsed by the EDPB.
[61] Article 35(7)(b) GDPR.
[62] Article 36(1) GDPR.
[63] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, footnote 60, paragraph 70.
[64] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, paragraph 68 and Recital 7 GDPR.

A.2.5 Where the same pods may be used by passengers consenting and not consenting to facial recognition, or when passengers not consenting to facial recognition may appear in the field of view while the system is not used, wait for a positive action from a consenting passenger before starting the capture of photo or video;

A.2.6 Possibility for a data subject, at any point in time, to perform deletion of data which is solely in their hands (biometric template[65]) as held in a mobile application or digital wallet[66] ;

A.2.7 Existence of viable alternatives or back-up solutions (i.e. for passengers who would not consent to the use of their biometric data, for passengers who would be unable to use such solutions, or for passengers suffering false rejections) so as also to ensure that the passengers who do not consent should not experience any detriment[67];

A.2.8 If using an application, it should be carefully designed and configured in order not to collect unnecessary data and to avoid the use of any third-party software development kits ("SDK") collecting data for other purposes.

A.3 Accountability

A.3.1 Assess whether any relevant codes of conduct or certification mechanisms exist to help demonstrate compliance with the security of processing in Article 32 GDPR[68]. Verify the appropriateness of the measures for the particular processing in question. Standards[69], best practices and codes of conduct, which are recognised by associations and other bodies representing categories of controllers, can be helpful in determining appropriate measures;

A.3.2 Ensure basic security checks are performed on the users' device to allow the enrolment phase, even though the passenger also has a role in the protection of their data as these are stored on their device. Examples of such technical checks and controls are presented below in section C.2 "Infrastructure and network".

B. Organisational:

B.1 Policy and compliance

B.1.1. Ensure that internal access controls are in place[70] with rules for administrators;

[65] References to biometric template in the safeguards for Scenario 1 correspond to references to the key/ secret in Scenario 2.
[66] Please note this safeguard only applies to Scenario 1.
[67] EDPB Guidelines 3/2019 on video devices, paragraph 86.
[68] Article 32(3) GDPR and EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, paragraph 10.
[69] See, for example, ISO/IEC 2382-37.
[70] EDPB Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020 (hereinafter "**EDPB Guidelines 4/2020 on location data and contact tracing tools**"), SEC-10, p. 16.

B.1.2 Where the facial recognition service can be provided by one of the parties involved in the processing without ID or biometric, or both kinds, of data, having to be handled by the other parties involved, forbid those data to flow through those other parties. For example, an airline company does not need to technically access the biometric data when it relies on the airport common infrastructure, even if this airline company acts as the controller of the processing under the GDPR;

B.1.3 Define a policy for encryption and key management[71], such as for the processing of ID and biometric data;

B.1.4 Ensure compliance with Chapter V GDPR. For example, to ensure compliant transfers if the controller uses a remote service during the enrolment process which is based in a third country;

B.1.5 When processors are used, ensure a processor agreement[72] in line with Article 28(3) GDPR is in place;

B.1.6 Ensure procedures are in place to manage human oversight and intervention, in particular to deal with false rejection issues and technical or usability issues.

B.2 Training and testing

B.2.1.Ensure personnel are trained in the appropriate manner;

B.2.2 Implement a "process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing"[73];

B.2.3. Implement a process to ensure that the processing of the passenger's biometric template[74] for authentication is technically effective and sufficiently accurate;

B.2.4. Ensure that biometric samples collected both at enrolment and at the checkpoint are of sufficient quality to perform a reliable biometric processing.

C. Technical:

C.1 Access

C.1.1 Implement safeguards during enrolment phase to ensure bootstrapping enrolment process with a verified identity. For example, to reinforce the assessment of users' identities

[71] EDPB Guidelines 3/2019 on video devices, paragraph 89.
[72] Article 28(3) GDPR.
[73] Article 32(1)(d) GDPR.
[74] References to biometric template in the safeguards for Scenario 1 correspond to references to the key/ secret in Scenario 2.

multifactor authentication, steps can be implemented, ranging from password protected one-time links to activate the app, to local device unblocking mechanisms;

C.1.2 Implement safeguards to address cases of false positive, presentation attacks and fraud prevention[75];

C.1.3 Prohibit any external access to the ID and biometric data[76];

C.1.4 Ensure that processing is done locally at enrolment, transmission and matching phases. The matching point should be as close as possible to the individual's device. Enabling the template matching within the individual device might require interaction with service providers located outside the airport and involving the use of public network resources, with the drawback of impacting availability and spreading the template to external entities;

C.1.5 Authenticate a user to add a new flight and generate a new encrypted QR code;

C.1.6 Implement measures to address the situation where a passenger may lose access to their QR code.

C.2 Infrastructure and network

C.2.1 Conditions on operating system ("OS") kept up-to-date and authentication being enabled for access to the device for the application/ digital wallet to work, including with automatic deletion of ID and biometric data if OS is outdated and poses security risks;

C.2.2 Isolation of matching units (i.e. pods) from network when operating and take all other necessary measures to ensure security;

C.2.3 Perform biometric matching on the passenger's device or on the pod (edge computing);

C.2.4 Solutions to address security vulnerabilities of passengers' individual devices including encryption of (at minimum) biometric and ID data at rest;

C.2.5 Utilise secure storage for (at least) biometric data solely at the hand of the user[77], for example by using a secure enclave on a smartphone;

C.2.6 Security safeguards to ensure the physical security of the premises, including the airport biometric terminal. Ensure a high level of security for the elements of the architecture which process (e.g. computation, data flow, transient or long-term storage) ID and biometric data.

[75] ENISA Report on Digital Identity on leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust of January 2022.
[76] EDPB Guidelines 3/2019 on video devices, paragraph 89.
[77] References to biometric template in the safeguards for Scenario 1 correspond to references to the key/ secret in Scenario 2.

C.3 User identity check data security and management

C.3.1 Compartmentalise data during transmission and storage in at least three different groups, such as: ID, biometric and flight details[78]. Ensure the data is appropriately encrypted between transmission and storage;

C.3.2 Put in place technical measures to ensure that only the data that can be processed lawfully at specific checkpoints are being processed and verified at the checkpoint;

C.3.3 Ensure the effectiveness of data deletion[79] through a secure deletion procedure (for example, main memory, cache, potential backups) and assess when deletion of the data should be automated. Data storage periods should be strictly enforced through automatic routines without needing a supplementary action from the individual[80];

C.3.4 Ensure the authenticity and integrity of the data (for example, signature)[81];

C.3.5 Retain passengers' biometric data at the enrolment point and at checkpoint only for a very short period and delete it as soon as the passenger has gone through the checkpoint;

C.3.6 If an application is used for the enrolment, apply security standards for mobile application security during the development of the application, as well as security tests by a third-party;

C.3.7 Ensure security measures are in place during the enrolment phase at the airport to preserve the confidentiality and integrity of the passenger's biometric data. For example, if the QR code is printed by the kiosk, the QR code should not be displayed at the kiosk to avoid a malicious actor taking a picture. In cases of short-range transmission, the transmission should be performed relying on user's active involvement and through a channel ensuring proximity;

C.3.8 Data which is solely at the hands of the individual[82] should be kept in a secure storage on the individual's device and any possible vulnerabilities related to the device's operating systems needs to undergo the appropriate security patches. In the case of a printed QR code, the individual should be made aware of the particular sensitive nature of the data it contains and what it allows to perform;

[78] EDPB Guidelines 3/2019 on video devices, paragraph 89.
[79] EDPB Guidelines 3/2019 on video devices, paragraph 89.
[80] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, paragraph 82.
[81] EDPB Guidelines 3/2019 on video devices, paragraph 89.
[82] References to biometric template in the safeguards for Scenario 1 correspond to references to the key/ secret in Scenario 2.

C.3.9 Ensure enrolment is performed following adequate remote identity proofing techniques[83].

3.2.2 Scenario 2: centralised storage of enrolled biometric template in an encrypted form within the airport and with a key/ secret solely in the passengers' hands, for authentication

48. This section examines the compatibility with Articles 5(1)(e) and (f), and Articles 25 and 32 GDPR of centralised storage, for authentication, of passengers' enrolled biometric templates in a centralised database, in an encrypted form and with a key/ secret held solely in the passenger's hands[84] (hereinafter "**Scenario 2**"). This section also examines the appropriate safeguards for Scenario 2, in light of Articles 25 and 32 GDPR.

Description of the Scenario

49. In Scenario 2, enrolment is done only once, for a given validity period (for instance, one year after the last flight, taken up to the expiration of passport validity), either remotely at appropriate identity assurance level (e.g. eIDAS appropriate level of assurance) or at airport terminals. The enrolment is controlled by the airport operator and consists in generating ID and biometric data that is encrypted with a key/ secret.

50. The database is stored within the airport premises, under the control of the airport operator. Individual-specific encryption keys/ secrets are stored only on the individual's device (for instance in the airport operator's mobile app). The app can generate a QR code containing the key/ secret, which may either be printed on paper or displayed on the device's screen[85]. Additionally, a second layer of encryption[86] is done by the airport operator with keys controlled by the airport operator.

51. Passengers are authenticated (1:1 comparison), when going through specific checkpoints at the airport. The passengers choosing to go through the biometric checkpoints show their QR code to a dedicated control pod equipped with a QR scanner and a camera. The passenger's index is sent to the database to request the encrypted template which is downloaded and checked locally on the pod and/ or user's device. Only the matching result is known to and used by the check point controller[87].

52. In this Scenario, there are no ID and biometric data flows between airports, with neither interconnection nor interoperability between the centralised databases.

EDPB's assessment

[83] See ENISA Report on Remote ID Proofing: Analysis of methods to carry out identity proofing remotely, March 2021.
[84] As exemplified by use case 2 in Annex I of the Request.
[85] The FR SA has further clarified there might also be other technical solutions to send the required information, such as by using a short-range communication protocol.
[86] The key/ secret (in the hands of the individual) is itself encrypted with another key held by the airport operator.
[87] The FR SA clarified that this storage period is illustrative and may be deemed as acceptable given that the key is held in the hands of the individuals and might be chosen at the enrolment phase. However, it should be noted that such storage period may be adjusted.

53. In Scenario 2, the passengers' enrolled biometric templates are stored in a centralised manner, but in an encrypted form and with a key/ secret solely held in the passengers' hands. In Scenario 2, the passengers are authenticated (1:1 comparison).

54. In this scenario, it is proposed that the goal of streamlining the passenger flow (i.e., by increasing the speed of checks) could be achieved with the use of a centralised system. The EDPB has previously noted that such solution could be considered as a viable alternative to the decentralised storage of the enrolled biometric templates[88] (as described in Scenario 1), if in presence of objective needs and with the use of appropriate safeguards (see safeguards described from paragraph 60 below).

55. In terms of security considerations, each individual's data is encrypted with the specific key kept only by the individual and under their sole control. Moreover, the fact that the information required for the matching (i.e. the secret/ key) needs to be given by the individual acts as a second factor[89] and thus reinforces the security of the authentication. Additionally, a second layer of encryption is done by the airport operator with keys controlled by the airport operator. In Scenario 2, the individual's index is sent to the central database in order to retrieve the biometric data associated with the individual. This data is then sent (encrypted) to a computer localised at the checkpoint where it is decrypted in order to perform the matching and only the matching result is known to and used by the checkpoint controller. Provided that the individual's key/ secret is kept in the computer localised at the checkpoint and that only a passenger's index is sent to the central database to recover the encrypted biometric template, such security measures could therefore be considered compatible with Articles 5(1)(f) and 32 GDPR.

56. Regarding the compatibility with Article 25 GDPR, and in particular in order to comply with the requirement of data minimisation, it should be ensured that the processing meets the necessity principle. In Scenario 2, the measures chosen could be considered to have met the necessity principle in relation to the purpose pursued (i.e., streamlining the passenger flow at airports) if, depending on the circumstances of the processing, the controller can demonstrate that there are no less intrusive alternative solutions that could achieve the same objective as effectively. In Scenario 2 the passengers would still have to show their device[90]. Nevertheless, the controller may be able to demonstrate that Scenario 2 speeds up the verification process when compared to the current situation which includes a human checking whether the name on the boarding pass matches the passenger's identity document[91] or when compared to Scenario 1. Notably, this could not be shown if there are currently no checks performed to verify the passengers' identity based on their official identity document (in this regard, see paragraph 18 above).

57. Regarding the proportionality principle, the intrusiveness from such processing can be counterbalanced by the active involvement of the passengers, who hold under their sole control the key to their encrypted data. Moreover, it appears that the security risks entailed by the storage of the passengers' biometric data in a centralised database and with the key solely in the passengers' hands can be mitigated with the use of appropriate safeguards (see safeguards addressed from

[88] EDPB Guidelines 3/2019 on video devices, paragraph 88.
[89] For example, this mitigates the risk of identity spoofing. See also safeguard C.1.2.
[90] The FR SA has further clarified there might also be other options to present a template, e.g. printed on paper. In addition, the EDPB recognises that in the future it could be envisaged to use an alternative technology, e.g. based on a near-field communication system.
[91] It could also be argued that the biometric check may be less prone to errors than compared to a human check.

paragraph 60 below). Therefore, assuming that the controller implements appropriate safeguards as required by the specific processing in question, the risks to individuals could be mitigated and the negative impact on the data subjects' fundamental rights and freedoms could be considered as proportional to the anticipated benefit. Of course, in each case it should be ensured that only the data needed for the purpose is processed and only passengers who consented would be checked, thus there is no risk that biometric data of other passengers, who did not consent, would be collected.

58. In the Request, it is stated as an example that, in Scenario 2, the storage period of the encrypted data in the database could be typically one year after the last flight taken by the individual and up to the expiration of passport validity. No information has been provided in the Request in order to substantiate such a long period based on objective reasons, although it can be presumed that such storage period is envisaged for convenience purposes for future flights. In terms of the storage period, in order to achieve compatibility with Article 5(1)(e) GDPR in this scenario, the controllers should be able to justify why this retention period is necessary for the purpose in specific cases. The Board recommends the controllers to envisage the shortest possible storage period, also taking into account passengers that fly only very rarely, and offer the data subjects to set their preferred storage period.

59. In light of these considerations, in reply to question 2.1.1 the Board concludes that such processing **could be considered to be in principle compatible with Articles 5(1)(e), 5(1)(f), 25 and 32 GDPR, subject to appropriate safeguards**.

Appropriate safeguards

60. In this type of scenario, in reply to question 2.1.2, the Board considers that, **in addition to the safeguards listed under Scenario 1**, at least the following safeguards should be implemented. *Other safeguards than the ones described in this Opinion could be used to achieve the same security and data protection goals and could be lawful as long as they ensure compliance with the applicable legal frameworks.*

61. Note: *this is a high level and non-exhaustive overview of the possible appropriate safeguards, which could be implemented by a controller in a solution similar to Scenario 2. Their appropriateness under Articles 25 and 32 GDPR will depend on a case-by-case analysis. All controllers will need to ensure that they conduct their own DPIA and their specific solutions may require additional measures not included in this Opinion.*

D. General

D.1 Data subject rights and safeguards that can be implemented by controllers

D.1.1 Ensure the passenger has control over the data storage periods for all of their data. The storage periods should be limited to what is necessary for the specific purpose. A maximum period should be set as a result of a thorough analysis of factors such as the validity of the identification document. The data subjects should be offered to set their preferred storage period, which could be shorter than the default storage period;

D.1.2 Possibility for a data subject at any point in time to request deletion of data which is solely in their hands (key/ secret) as held in a mobile application or digital wallet[92];

D.1.3 Ensure the localisation of the central database allows an effective supervision by the competent supervisory authority.

E. Organisational:

E.1 Policy and compliance

E.1.1 Trust in the central server must be limited. Ensure the management of the central server follows clearly defined governance rules and includes all necessary measures to ensure its security[93].

F. Technical:

F.1 Access

F.1.1 Maintain logs of who has access to personal data, in particular ID and biometric data, and when it was accessed;

F.2 Infrastructure and network

F.2.1 Appropriately secure the central database, including against availability attacks;

F.2.2 Ensure there is no internet connection to the central database, the enrolment pods and matching units. Operation and maintenance of these system (e.g. backup, patching, monitoring, etc.) are to be performed locally within the airport premises.

F.3 Data Security and management

F.3.1 Implement state of the art cryptographic techniques to secure exchanges between the application and the centralised server[94];

F.3.2 Keep the individual key/ secret at the level where it will be used to decrypt (i.e. in the pod) and only use the index to recover the corresponding enrolled biometric template in the central database;

F.3.3 Ensure the key/ secret interchange between user device and pod protects the communication against any possible eavesdropping or transmission to third parties;

[92] Please note this safeguard only applies to Scenario 2.
[93] EDPB Guidelines 4/2020 on location data and contact tracing tools, PRIV-5, p. 17.
[94] EDPB Guidelines 4/2020 on location data and contact tracing tools, SEC-4 p. 16: "Examples of techniques that can be used include for example: symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, homomorphic encryption".

F.3.4 Index the biometric template when stored in the central database to allow for 1:1 authentication and ensure it is unique and related to the individual. Ensure the index does not reveal any of the passenger's ID information and is not correlated with the encryption key;

F.3.5 Appropriately authenticate and encrypt any transmission between the central database and checkpoints and put it on isolated networks;

F.3.6 Avoid bidirectional links between sets of data (ID and biometric data, as well as flight details) and keep only relevant unidirectional links in the database. For example, only the unidirectional links from index to ID, from index to encrypted biometric data, and from index to flight details;

F.3.7 Ensure business continuity arrangements, such as by having appropriate back-up storage systems in place;

F.3.8 Ensure the pod does not keep logs of the encrypted or unencrypted templates.

3.2.3 Centralised storage of the enrolled biometric templates for identification

62. This section examines the compatibility with Articles 5(1)(e) and (f), and Articles 25 and 32 GDPR of centralised storage, for identification, of the passengers' enrolled biometric templates, where such templates are not encrypted with a key/ secret held solely in passengers' hands, in two use cases: (1) when such templates are stored in a database within the airport, under the control of the airport operator[95] (hereinafter "**Scenario 3.1**"), and (2) when such templates are stored in the cloud, under the control of the airline company[96] (hereinafter "**Scenario 3.2**").

63. The Board considers that the use of biometric data for **identification** purposes in large central databases interfere with the fundamental rights of data subjects and could possibly entail serious consequences for data subjects[97]. In addition, the use of biometric data should also be examined in relation to the purpose for which it is processed, in light of the necessity and proportionality principles[98].

3.2.3.1 Scenario 3.1: centralised storage in a database within the airport, under the control of the airport operator

Description of the Scenario

64. In Scenario 3.1, the passengers' enrolled biometric template is stored in a central database at the airport premises and under the control of the airport operator in an encrypted form. In particular, the

[95] As exemplified by use case 3A in Annex I of the Request.
[96] As exemplified by use case 3B of Annex I of the Request.
[97] For example, see Article 29 WP Opinion 3/2012 on biometric technologies, p. 8. See also paragraph 26 above.
[98] Recital 4 GDPR. See also Article 29 WP Opinion 3/2012 on biometric technologies, p. 8.

passengers' data is compartmentalised, meaning that their ID data, enrolled biometric template and flight information is stored in three different databases. Such data is encrypted with different keys, both during storage and while being transmitted to the servers performing the matching, where it is then decrypted by the airport operator.

65. The passengers need to enroll for each flight, in a short period before their departure (e.g. 48 hours). Such enrolment may be performed either remotely or at airport terminals at an appropriate identity assurance level (e.g. eIDAS appropriate level of assurance). Alternatively, the enrolment can take the same form as described in Scenario 1, in which case the passengers need to push their data from their digital wallets to the airport system within a 48-hour timeframe prior to their departure.

66. In this scenario too, the passengers present themselves before a dedicated control pod equipped with a camera. Their biometric sample is then sent to a central airport server, which will attempt to match the data with that of the central biometric database. The passenger can thus be identified and checked for whether or not they are indeed registered for a departing flight (or the boarding flight in case of control at boarding). Depending on the checkpoint, the data sent back to the requesting checkpoint controller may be minimised, for example as a "yes/ no reply" or the matching result itself, if necessary. In this case, only the request result is transmitted to and used by a checkpoint controller.

67. In particular, in this scenario the passengers are identified (1:N comparison), where N is the number of passengers expected at the airport in a timeframe of several days. Moreover, the biometric matching is only performed when each passenger presents themselves at pre-defined control points at the airport of departure, but the data processing itself is done at a central server connected to the central database. The storage period in this scenario is typically 48 hours and data is deleted once the plane has taken off.

EDPB's assessment

68. As recalled above, the processing of biometric data entails heightened risks to data subjects' rights and freedoms[99]. Thus, any failure in data security may have particularly severe consequences for data subjects[100]. Controllers are obliged to effectively mitigate those risks. Since in this scenario the entire architecture is completely centralised, the passengers lose control of their data to a greater extent. Furthermore, the risk that the data ends up being processed for other purposes different from the control of passengers' flow could also be greater.

69. In light of the principle and requirements on security (Article 5(1)(f) and 32 GDPR), it should be considered that the storage of ID and biometric data in central, albeit separate, databases may provide high value points of attack and a breach of confidentiality of such database may subsequently entail access to the whole set of data. As a consequence, a possible breach concerning facial recognition templates and associated ID may enable the unauthorised or unlawful identification of the data subjects in other environments. It may also, depending on the methods used for biometric identification, threaten the further safe use of facial recognition templates as an identifier. In that

[99] See paragraph 26 above.
[100] Guidelines on facial recognition, Consultative Committee of Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data, June 2021, p. 22.

case, the effects of the breach cannot be mitigated, unlike the case of another type of credential (e.g. user ID, password) that are possible to change[101].

70. Additionally, the high quantity and quality of ID and biometric data held by the controller makes it a very valuable target for an attacker, which entails, in terms of security risk, a higher level of likelihood. Furthermore, data breaches could have greater impact as, due to the storage of data in a centralised location, it could be easier for attackers to gain access to personal data relating to multiple passengers. Therefore, a possible breach could potentially expose a large number of data subjects to high risks in terms of severity, for instance identity theft on a large scale, that are extremely difficult to mitigate.

71. Therefore, regarding compatibility with Article 5(1)(f) and Article 32 GDPR, the measures envisaged in Scenario 3.1[102], taking into account the state of the art, are insufficient to ensure a level of security appropriate to the risk. On this basis, the processing under Scenario 3.1 would not comply with Article 5(1)(f) and Article 32 GDPR if a controller would limit themselves to those measures.

72. In light of the principle of Article 5(1)(e) GDPR, in this Scenario, the biometric data storage period in the central database is typically 48 hours. Such storage limitation seems to significantly reduce risks associated with personal data breaches. Nevertheless, the data storage period is not a decisive factor, on its own merit, for the overall compatibility of said architecture, as such retention periods may be subject to changes by the controllers. In any event, the proposed measures need to comply with the requirements of data protection by design and by default under Article 25 GDPR.

73. In contrast to Scenarios 1 and 2, where the passengers are authenticated, in Scenario 3.1, the passengers are identified (1:N comparison), where N is the number of passengers expected at the airport in a timeframe of several days who have consented to such processing when going through specific checkpoints at the airport. This implies the search of passengers within a central database, by processing each biometric sample captured to check whether it matches with a person known to the system. In contrast to Scenario 2, in Scenario 3.1, the keys are not held solely in the passengers' hands. Consequently, in this scenario, the passengers have significantly less control over their biometric data. Therefore, such processing as proposed under Scenario 3.1 cannot be compatible with data protection by design and design requirements under Article 25 GDPR.

74. In the light of Article 25 GDPR, controllers should consider the types, categories and level of detail of personal data required for the processing purposes[103]. Their design choices should take into account the increased risks to the principles of data minimisation, integrity and confidentiality and storage limitation when collecting large amounts of detailed personal data, and compare it to the reduction in risks when collecting smaller amounts and/ or less detailed information about data subjects. In any case, the default setting should not include collection of personal data that is not necessary for the specific processing purpose. In other words, if certain categories of personal data are unnecessary or if detailed data is not needed because less granular data is sufficient, then any surplus personal data should not be collected. In this case, if another processing implementation could achieve the same objective and is available as per the terms described in Scenario 3.1, it is not necessary to use facial recognition technology.

[101] See in this regard, A29WP Opinion 3/2012 on biometric technologies, p. 34.

[102] As described in paragraphs 64-67 above.

[103] EDPB Guidelines 4/2019 on Data Protection by Design and by Default, paragraph 49.

75. Regarding Article 25 GDPR, a key data protection by design and default element is the autonomy of the data subject. In particular, the data subject should be granted the highest degree of autonomy as possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing[104]. In Scenario 1, the data subject would have autonomy and control regarding the use, disclosure, and erasure of their biometric templates and, in Scenario 2, the data subject would maintain some control regarding the disclosure of their own biometric template, as they encryption key/ secret would be stored in their hands. However, in Scenario 3.1 the data subject is fully dependent on the controller's choices regarding the processing of their biometric data and therefore has no direct control regarding the use of their biometric template.

76. Regarding the compatibility with Article 25 GDPR, and in particular in order to comply with the requirement of data minimisation, the processing envisaged in Scenario 3.1 cannot meet the necessity principle. The Board considers that a similar result to streamline the passenger flow at airports can be achieved in a less privacy intrusive manner. For instance, this can be achieved without the use of biometric data (although the user experience would then be different, as it might take longer to show their boarding pass and, where needed, official identification documents). Furthermore other solutions, notably those relying on the storage of the biometric data in a local wallet on the individual's device or those requiring encryption of the data with a specific key stored in the individual's device, allow to reach the objectives in a less privacy intrusive manner.

77. Regarding the proportionality principle, the processing envisaged in Scenario 3.1 would create risks to the rights of the data subjects that would not be mitigated by the envisaged measures given the state of the art. The risk of a negative impact on the data subjects' fundamental rights and freedoms that could result from a data breach in a centralised database of biometric data of a large number of individuals seems to outweigh the anticipated benefit resulting from the processing, as such benefit is relatively minor, i.e. a slight increase in convenience and speed of the checks. Therefore, it cannot justify the high intrusiveness of those measures for the fundamental rights and freedoms of individuals and the processing envisaged in Scenario 3.1 does not meet the proportionality principle.

78. In light of these considerations, in reply to question 2.2.1 the Board concludes that, when the processing is done for the specific purpose of streamlining the passenger flow at airports, the processing envisaged in Scenario 3.1:

- **cannot be compatible with Article 25 GDPR**;
- **would not comply with Article 5(1)(f) and Article 32 GDPR** if a controller would limit themselves to the measures as described in Scenario 3.1.

[104] EDPB Guidelines 4/2019 on Data Protection by Design and by Default, paragraph 70. Recital 7 GDPR further clarifies that "[n]atural persons should have control of their own personal data".

3.2.3.2 Scenario 3.2: centralised storage in a cloud, under the control of the airline company

Description of the Scenario

79. In Scenario 3.2, the passengers' enrolled biometric template is stored in the cloud, under the control of the airline company or its cloud service provider (data processor). In the Request, it is specified that the cloud service provider would be located in the EEA[105]. In this case, the passengers' data is encrypted, but decrypted when in use (for instance, when the matching operation is performed), and the keys are controlled by the airline company or its cloud processor. The passengers' biometric data is used for the passengers' identification (1:N comparison), where N is potentially up to the number of total customers of the airline company[106].

80. Similarly to the scenarios 1, 2 and 3.1, here too the passengers first need to enrol. However, in Scenario 3.2, the passengers' enrolment is done once, for as long as the customer holds an account with the airline company. The enrolment is done either in a remote mode at appropriate identity assurance level (e.g. eIDAS appropriate level of assurance) or at airport terminals. The biometric matching is only performed when the passengers present themselves at pre-defined control points at the airport, but the data processing itself is done in the cloud.

81. At the airport, the passengers go through dedicated control pods, equipped with a camera. The passengers' biometric data is sent through a request to an airline cloud server, where the matching of this data is performed against the central database. The passenger can thus be identified and checked for whether or not they are indeed registered for a departing flight (or the boarding flight in case of control at boarding).

82. Potentially, matching results can be made available to multiple airport operators where an airline company has a dedicated terminal or access to an airport's common information system infrastructure. Depending on the checkpoint, the data sent back to the requesting checkpoint controller may be minimised, for example as a "yes/ no reply" or the matching result itself, if necessary. In this case, only the request result is known to and used by the checkpoint controller.

83. The storage period of the template is defined by the airline company and can potentially last as long as the customer has an account with the airline company.

EDPB's assessment

84. The considerations already expressed by the Board in relation to Scenario 3.1[107] also apply for this Scenario.

85. Regarding the principle and requirements on security (Articles 5(1)(f) and 32 GDPR), the processing in Scenario 3.2 is done in the cloud and multiple entities could have access to such data, including

[105] The FR SA clarified that this is illustrative and that cloud service providers which are not located in the EEA could also be envisaged. In addition, other storage solutions (e.g. without use of cloud) could also be envisaged.
[106] The FR SA clarified that this is illustrative and there is a solution where biometric data is pushed each time in advance of the flight.
[107] Paragraphs 68-77 above.

possibly non-EEA providers, even when the data is held in the EEA[108]. Such architecture entails potential risks concerning transfers of personal data to third countries. In addition, although the passengers' data is encrypted, it is decrypted when in use (i.e. when the matching operation is performed), while the keys are controlled by the airline company or its cloud processor. Such storage may lead to a further increase in the security exposure surface.

86. Therefore, regarding compatibility with Article 5(1)(f) and Article 32 GDPR, the measures envisaged in Scenario 3.2[109], taking into account the state of the art, are insufficient to ensure a level of security appropriate to the risk. On this basis, the processing under Scenario 3.2 would not comply with Article 5(1)(f) and Article 32 GDPR if a controller would limit themselves to those measures.

87. In addition, according to Scenario 3.2[110], the data could be stored for a significant period (i.e. potentially lasting as long as the data subject has an account with the airline company). Such storage duration exposes the data to higher risks of a breach to their confidentiality and integrity and seems to go beyond what is strictly necessary and proportionate for the purposes of the processing. The Board notes that the data storage period is not a decisive factor, on its own merit, for the overall compatibility with the GDPR of the said architecture, as it may be subject to changes by the data controllers. However, based on the information available to the Board and contained in the description of Scenario 3.2, there is not a sufficient justification for this lengthy retention period and no apparent measures to mitigate the risks to individuals. Based on this, the proposed storage period would not be limited to what is necessary, pursuant to the storage limitation principle in Article 5(1)(e) GDPR.

88. In any event, the proposed measures in Scenario 3.2 cannot satisfy the data protection by design and design requirements of Article 25 GDPR. In Scenario 3.2, the passengers' enrolled biometric templates are stored in the cloud, under the control of the airline company or its cloud service provider (data processor). As described above, multiple entities could potentially have access to this data. Furthermore, the passengers' biometric data is used for the passengers' identification (1:N comparison), where N is potentially up to the number of total users/customers of the airline company. Such method entails finding a person among a group of individuals within the central database, by processing each captured face to check whether it matches with a person known to the system. In contrast to Scenario 3.1, in Scenario 3.2 the comparison could be performed in a much larger scale, as the criterion here is the number of total customers of the airline company, while Scenario 3.1 only included the number of passengers expected in a timeframe of several days.

89. Moreover, regarding the compatibility with Article 25 GDPR, and in particular in order to comply with the requirement of data minimisation, the processing envisaged in Scenario 3.2 cannot meet the necessity principle. The Board considers that a similar result to streamline the passenger flow at airports could be achieved by other less intrusive measures, for instance without the use of biometric data, although the user experience would then be different as it might take longer to show their ID and boarding pass. Furthermore, other solutions, notably those relying on the storage of the biometric data in a local wallet on the individual's device or those requiring encryption of the data with a specific

[108] EDPB 2022 Coordinated Enforcement Action on the use of cloud-based services by the public sector of 17 January 2023, p. 19.
[109] See paragraphs 79-83 above.
[110] See above paragraph 83.

key stored in the individual's device, allow the controller to reach the objectives in a in a less privacy intrusive manner.

90. Regarding proportionality principle, the processing envisaged in Scenario 3.2 would create risks to the rights of the data subjects that would not be mitigated by envisaged safeguards. The negative impact on the data subjects' fundamental rights and freedoms that would result from a data breach in a centralised database of biometric data of a large number of individuals stored in the cloud seems to outweigh the anticipated benefit resulting from the processing, as such benefit is relatively minor, i.e. a slight increase in convenience and speed of the checks. Therefore, it cannot justify the high intrusiveness of those measures for the fundamental rights and freedoms of individuals and the processing envisaged in Scenario 3.2 cannot be considered proportionate.

91. In light of these considerations, in reply to question 2.3.1, the Board concludes that, when the processing is done for the specific purpose of streamlining the passenger flow at airports, the processing envisaged in Scenario 3.2:

- **cannot be compatible with Article 25 GDPR**;
- **would not comply with Article 5(1)(f) and Article 32 GDPR** if a controller would limit themselves to the measures as described in Scenario 3.2;
- **would not comply with Article 5(1)(e) GDPR**, as there is not a sufficient justification for the retention period envisaged in Scenario 3.2, based on the information available to the Board. In order to comply with the storage limitation principle in Article 5(1)(e) GDPR, the controller would need to demonstrate that personal data are stored no longer than necessary for the purposes for which they are processed.

4 CONCLUSIONS

92. Regarding the question 1.1, on the basis of the request for an opinion from the FR SA, in relation to the requirements of Articles 5(1)(f), 25 and 32 GDPR, and on the basis of the analysis above, the Board concludes that:

93. the use of facial recognition technology for biometrics-enabled authentication, for the specific purpose of streamlining the passenger flow at airports (security checkpoints, baggage drop-off, boarding and access to passenger lounge) could be considered to be in principle compatible with the principles of integrity and confidentiality under Article 5(1)(f), Articles 25 and 32 GDPR, in the case of a storage architecture, where the enrolled biometric template of each passenger is stored locally on their individual device and under their sole control, if subject to appropriate safeguards as described from paragraph 46 above.

94. Regarding the question 2.1.1, on the basis of the request for an opinion from the FR SA, in relation to the requirements of Article 5(1)(e) and (f), and Articles 25 and 32 GDPR, and on the basis of the analysis above, the Board concludes that:

95. the use of facial recognition technology for biometrics-enabled authentication, for the specific purpose of streamlining the passenger flow at airports (security checkpoints, baggage drop-off, boarding and access to passenger lounge) could be considered to be compatible in principle with the principle of storage limitation under Article 5(1)(e) and the principles of integrity and confidentiality under Article 5(1)(f), and Articles 25 and 32 GDPR in the case of a centralised storage architecture, where the enrolled biometric template of each passenger is stored in a central database within the

airport, under the control of the airport operator, in an encrypted form, with a key/ secret held solely in the hands of the individual, if subject to appropriate safeguards as described from paragraph 60 above.

96. Regarding the question 2.2.1, on the basis of the request for an opinion from the FR SA in relation to the requirements of Article 5(1)(e) and (f), and Articles 25 and 32 GDPR and on the basis of the analysis above, the Board concludes that:

97. the use of facial recognition technology for biometrics-enabled identification, used for the specific purpose of streamlining the passenger flow at airports (security checkpoints, baggage drop-off, boarding and access to passenger lounge) in the case of a centralised storage architecture, when the passengers' enrolled biometric templates are not encrypted with a key/ secret held solely in each passenger's hands, where such templates are stored in a database within the airport (under the control of the airport operator), cannot be compatible with Article 25 GDPR. Also, such processing would not comply with the principle of integrity and confidentiality under Article 5(1)(f) and Article 32 GDPR, if a controller would limit themselves to the measures as described in Scenario 3.1.

98. Regarding the question 2.3.1, on the basis of the request for an opinion from the FR SA in relation to the requirements of Article 5(1)(e) and (f), and Articles 25 and 32 GDPR and on the basis of the analysis above, the Board concludes that:

99. the use of facial recognition technology for biometrics-enabled identification, used for the specific purpose of streamlining the passenger flow at airports (security checkpoints, baggage drop-off, boarding and access to passenger lounge) in the case of a centralised storage architecture, when the passengers' enrolled biometric templates are not encrypted with a key/ secret held solely in each passenger's hands, where such templates are stored in the cloud (under the control of the airline company) cannot be compatible with Article 25 GDPR. Also, such processing would not comply with the principles of integrity and confidentiality under Article 5(1)(f) and Article 32 GDPR, if a controller would limit themselves to the measures as described in Scenario 3.2. Finally, based on the description of Scenario 3.2 and the information available to the Board, the processing would not comply with the principle of storage limitation under Article 5(1)(e) GDPR.

For the European Data Protection Board

The Chair

(Anu Talus)