
# Avis 11/2024 sur l'utilisation des technologies de reconnaissance faciale pour rationaliser le flux de passagers dans les aéroports [compatibilité avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD]

## Version 1.1

## Adopté le 23 mai 2024

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

| | | |
|---|---|---|
| Version 1.1 | 28 mai 2024 | Correction grammaticale dans la synthèse (pages 3 et 4) et les points 77 et 90 de l'avis |
| Version 1.0 | 23 mai 2024 | Adoption de l'avis |

**Synthèse**

L'autorité de contrôle française a demandé au comité européen de la protection des données (ci-après l'«EDPB» ou le «comité») d'émettre un avis sur l'utilisation des technologies de reconnaissance faciale par les exploitants d'aéroport et les compagnies aériennes pour l'authentification ou l'identification biométrique des passagers dans le but de rationaliser le flux de passagers dans les aéroports.

À titre liminaire, le comité rappelle que l'utilisation de données biométriques, et de la technologie de reconnaissance faciale en particulier, présente des risques accrus pour les droits et libertés des personnes concernées. Elle se rapporte au traitement des données biométriques qui bénéficient d'une protection spéciale en vertu de l'article 9 du RGPD. Avant d'utiliser de telles technologies, même si celles-ci devaient être considérées comme particulièrement efficaces, les responsables du traitement devraient évaluer leur incidence sur les libertés et droits fondamentaux des personnes concernées et examiner si la finalité légitime du traitement peut être atteinte par des moyens moins intrusifs.

Le champ d'application du présent avis, conformément à la demande, est limité à la compatibilité du traitement avec l'**article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD** dans le **but spécifique de rationaliser le flux de passagers dans les aéroports** à quatre points de contrôle spécifiques, à savoir aux points de contrôle de sûreté, au point de collecte des bagages, à l'embarquement et à l'accès au salon des passagers. Le présent avis ne propose pas d'analyse complète et exhaustive du respect du RGPD par le ou les responsables du traitement concernés dans chaque cas, ainsi que par leur(s) sous-traitant(s), le cas échéant. Il est donc sans préjudice d'une analyse juridique et technique au cas par cas fondée sur les circonstances propres à un responsable du traitement et le traitement spécifique envisagé par celui-ci. Par ailleurs, l'analyse de la base juridique applicable n'entrant pas dans le champ des questions soumises au comité dans la demande, la validité du consentement pour un tel traitement, au regard des articles 6, 7 et 9 du RGPD, n'est pas examinée dans le présent avis. Cet avis est également sans préjudice des restrictions à l'utilisation des données biométriques prévues par le droit des États membres.

Dans le présent avis, le comité évalue la conformité du traitement avec les dispositions susmentionnées du RGPD dans le contexte de **quatre scénarios spécifiques**.

Dans le **premier scénario**, le modèle biométrique inscrit est conservé par la personne elle-même, par exemple sur son appareil personnel, sous son contrôle exclusif, en vue de l'authentification (comparaison un à un) du passager lors de son passage par les points de contrôle susmentionnés de l'aéroport.

Le comité conclut que les mesures choisies pourraient être considérées comme conformes au principe de nécessité si le responsable du traitement peut démontrer qu'il n'existe pas d'autres solutions moins intrusives qui permettraient d'atteindre le même objectif de manière aussi efficace. En outre, le caractère intrusif du traitement peut être compensé par la participation active des passagers, dès lors que leur modèle biométrique est conservé par eux seuls, par exemple sur leur appareil personnel, sous leur contrôle exclusif, et que leurs données sont effacées aussitôt la correspondance établie. Sur cette base, le comité conclut que le traitement envisagé dans le premier scénario **pourrait être considéré, en principe, comme compatible avec l'article 5, paragraphe 1, point f), et les articles 25 et 32, du RGPD**, sous réserve de la mise en œuvre de garanties appropriées.

Le comité a défini des garanties minimales qui devraient être mises en œuvre pour une solution similaire au premier scénario.

Le **deuxième scénario** envisage la conservation centralisée, au sein de l'aéroport, d'un modèle biométrique inscrit sous une forme cryptée et dont le passager est le seul à détenir la clé/le secret. Ce système permet l'authentification du passager (comparaison un à un) lors de son passage par les points de contrôle susmentionnés de l'aéroport. L'inscription est valable pour une période donnée qui, par exemple, pourrait être d'un an après le dernier vol et aller jusqu'à la date d'expiration du passeport.

Le comité conclut que le traitement pourrait être considéré comme conforme au principe de nécessité si le responsable du traitement peut démontrer qu'il n'existe pas d'autres solutions moins intrusives qui permettraient d'atteindre le même objectif de manière aussi efficace. En outre, le caractère intrusif du traitement peut être compensé par la participation active du passager, dès lors qu'il détient sous son contrôle exclusif la clé/le secret pour accéder à ses données biométriques cryptées. À supposer que le responsable du traitement mette en œuvre des garanties appropriées, les risques de sécurité liés à l'utilisation d'une base de données centralisée dans ce scénario pourraient être atténués et l'incidence négative sur les libertés et droits fondamentaux des personnes concernées pourrait être considérée comme proportionnée au bénéfice escompté. En ce qui concerne le principe de limitation de la conservation, aucune information n'a été fournie au comité pour justifier la longue durée de conservation. Afin d'assurer la compatibilité avec l'article 5, paragraphe 1, point e), du RGPD dans ce scénario, les responsables du traitement devraient être en mesure de justifier la nécessité de la durée de conservation envisagée au regard de l'objectif visé dans des cas spécifiques. Le comité recommande aux responsables du traitement d'envisager la durée de conservation la plus courte possible tout en offrant aux passagers la possibilité de fixer la durée de conservation de leur choix. Sur cette base, le comité conclut que le traitement envisagé dans le deuxième scénario **pourrait être considéré, en principe, comme compatible avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD**, sous réserve de la mise en œuvre de garanties appropriées.

Le comité a défini des garanties minimales qui devraient être mises en œuvre pour une solution similaire au deuxième scénario.

Le **troisième scénario** envisage la conservation centralisée d'un modèle biométrique inscrit sous une forme cryptée au sein de l'aéroport, sous le contrôle de son exploitant. Ce système permet l'identification des passagers (comparaison 1 à n) lors de leur passage par les points de contrôle susmentionnés de l'aéroport. Dans ce scénario, la durée de conservation est généralement de 48 heures et les données sont effacées aussitôt après le décollage de l'avion.

Étant donné que les données d'identification et les données biométriques sont conservées dans une base de données centrale, toute atteinte à la confidentialité de cette base de données pourrait ensuite ouvrir l'accès à l'ensemble des données et permettre l'identification non autorisée ou illicite des passagers dans d'autres environnements. L'architecture de stockage centralisée sous le contrôle de l'exploitant de l'aéroport a également pour effet de limiter davantage le contrôle des passagers sur leurs données. Le comité estime qu'un résultat semblable à la rationalisation du flux de passagers dans les aéroports peut être obtenu par des moyens moins intrusifs, et que l'incidence négative sur les libertés et droits fondamentaux des personnes concernées qui résulterait d'une violation des données dans une base de données centralisée contenant des données biométriques semble l'emporter sur le bénéfice escompté du traitement. Dès lors, le traitement ne saurait être conforme aux principes de nécessité et de proportionnalité. Sur cette base, le comité conclut que le traitement envisagé dans le troisième scénario **ne peut être compatible avec l'article 25 du RGPD**. En outre, il **ne serait conforme ni à l'article 5, paragraphe 1, point f), ni à l'article 32 du RGPD** si un responsable du traitement se limitait aux mesures décrites dans ce scénario.

Le **quatrième scénario** prévoit la conservation centralisée d'un modèle biométrique inscrit sous une forme cryptée dans le nuage, sous le contrôle de la compagnie aérienne ou de son fournisseur de services en nuage. Ce système permet l'identification des passagers (comparaison 1 à n) lors de leur passage par les points de contrôle susmentionnés de l'aéroport. Dans ce scénario, les données peuvent être conservées aussi longtemps que le client détient un compte auprès de la compagnie aérienne.

Étant donné que les données d'identification et les données biométriques sont conservées dans une base de données centrale dans le nuage, plusieurs entités pourraient avoir accès à ces données, y compris potentiellement des fournisseurs établis en dehors de l'EEE. Les données des passagers sont décryptées lorsqu'elles sont utilisées, et les clés d'accès sont sous le contrôle de la compagnie aérienne ou de ses sous-traitants, ce qui pourrait accroître l'exposition aux risques de sécurité. Cette architecture de stockage centralisée a également pour effet de limiter davantage le contrôle des passagers sur leurs données. Celles-ci pourraient également être conservées pendant une longue durée, ce qui les expose à un risque accru d'atteinte à la sécurité et semble excéder ce qui est strictement nécessaire et proportionné aux fins du traitement, à moins que d'autres mesures visibles ne soient prises pour atténuer les risques pour les personnes.

Le comité estime qu'un résultat semblable à la rationalisation du flux de passagers dans les aéroports peut être obtenu par des moyens moins intrusifs, et que l'incidence négative sur les libertés et droits fondamentaux des personnes concernées qui résulterait d'une violation des données dans une base de données centralisée contenant des données biométriques semble l'emporter sur le bénéfice escompté du traitement. Dès lors, le traitement ne saurait être conforme aux principes de nécessité et de proportionnalité. Sur cette base, le comité conclut que le traitement envisagé dans le quatrième scénario **ne peut être compatible avec l'article 25 du RGPD**. En outre, il **ne serait conforme ni à l'article 5, paragraphe 1, point e), du RGPD**, sur la base des informations dont dispose le comité, **ni à l'article 5, paragraphe 1, point f), et à l'article 32, du RGPD**, si un responsable du traitement se limitait aux mesures décrites dans ce scénario.

Table des matières

**Le Comité européen de la protection des données**

vu l'article 63 et l'article 64, paragraphe 2, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «**RGPD**»),

vu l'accord sur l'Espace économique européen, et notamment son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 10 et 22 du règlement intérieur du Comité européen de la protection des données (ci-après le «**comité**» ou l'«**EDPB**»),

considérant ce qui suit:

1) le rôle principal du comité consiste à garantir l'application harmonieuse du RGPD dans l'ensemble de l'Espace économique européen (ci-après l'«**EEE**»). L'article 64, paragraphe 2, du RGPD dispose que toute autorité de contrôle, le président du comité ou la Commission européenne peuvent demander que toute question d'application générale ou produisant des effets dans plusieurs États membres de l'EEE soit examinée par le comité en vue d'obtenir un avis.

2) l'avis du comité est adopté, conformément à l'article 64, paragraphe 3, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur de l'EDPB, dans un délai de huit semaines après que le président et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision du président, ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

**a adopté l'avis suivant:**

# 1 INTRODUCTION

## 1.1 Résumé des faits

1. Le 16 février 2024, l'autorité de contrôle française a demandé au comité d'émettre un avis sur la compatibilité avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD de l'utilisation de la technologie de reconnaissance faciale par les exploitants d'aéroport et les compagnies aériennes pour l'authentification ou l'identification biométriques des passagers[2] dans le but de rationaliser le flux de passagers, aux points de contrôle de sûreté de l'aéroport[3], au point de collecte des bagages, à l'embarquement et à l'accès au salon des passagers (à l'exclusion du contrôle aux frontières et des vérifications effectuées par les magasins hors taxes) (ci-après la «**demande**»).

[1] Dans le présent avis, on entend par «**États membres**» les États membres de l'EEE, et on entend par «Union» ou «UE» l'«EEE».

[2] Dans le contexte du présent avis, on entend par «**passager**» une personne concernée dont les données à caractère personnel sont traitées aux fins spécifiques décrites dans cet avis. Ci-après, les termes «passager» et «personne» sont utilisés de manière interchangeable.

[3] Aux fins du présent avis, les «**points de contrôle de sûreté de l'aéroport**» désignent les contrôles de sûreté effectués sous la responsabilité de l'exploitant de l'aéroport auxquels les passagers doivent se soumettre pour accéder à la zone d'embarquement ou à la porte d'embarquement depuis le hall des départs.

L'autorité de contrôle française a joint à sa demande une description de cas d'utilisation types (annexe I).

2. Dans sa demande, l'autorité de contrôle française fait observer que les modèles expérimentés actuellement dans plusieurs aéroports de l'Union varient d'un État membre à l'autre, ce qui risque de donner lieu à des divergences d'interprétation entre les autorités de contrôle et à des différences dans les effets sur les libertés et droits fondamentaux des personnes concernées dans l'UE[4].

3. Le comité estime que, pour pouvoir apporter une réponse à la demande, il est nécessaire de répondre aux questions suivantes:

4. **Question 1**:

1.1. L'utilisation de la technologie de reconnaissance faciale pour l'authentification biométrique **dans le but spécifique de rationaliser le flux de passagers dans les aéroports** (points de contrôle de sûreté, point de collecte des bagages, embarquement et accès au salon des passagers) peut-elle être compatible avec **l'article 5, paragraphe 1, point f), et les articles 25 et 32 du RGPD**, dans le cas d'une architecture de stockage dans laquelle le modèle biométrique de chaque passager est conservé **exclusivement par la personne elle-même**, par exemple localement sur son appareil personnel, sous son contrôle exclusif?

1.2. Si un tel traitement était jugé compatible avec les dispositions susmentionnées, quelles garanties minimales appropriées seraient nécessaires, à la lumière des articles 25 et 32 du RGPD?

**Question 2**:

2.1. L'utilisation de la technologie de reconnaissance faciale pour l'authentification ou l'identification biométriques **dans le but spécifique de rationaliser le flux de passagers dans les aéroports** (points de contrôle de sûreté, point de collecte des bagages, embarquement et accès au salon des passagers) peut-elle être compatible avec **l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD** dans le cas d'une architecture de stockage **centralisée**, dans laquelle le modèle biométrique de chaque passager est conservé dans une base de données centrale:

2.1.1. située au sein de l'aéroport, sous le contrôle de l'exploitant de l'aéroport, sous une forme cryptée, la clé/le secret étant détenu par le seul passager (par exemple sur son téléphone portable), aux fins de l'authentification?

2.1.2. si un tel traitement était jugé compatible, quelles garanties minimales appropriées seraient nécessaires, à la lumière des articles 25 et 32 du RGPD?

2.2.1. située au sein de l'aéroport, sous le contrôle de l'exploitant de l'aéroport, sous une forme cryptée, les clés étant détenues par ledit exploitant, aux fins de l'identification?

2.2.2. si un tel traitement était jugé compatible, quelles garanties minimales appropriées seraient nécessaires, à la lumière des articles 25 et 32 du RGPD?

[4] Demande, p. 1.

2.3.1. dans le nuage, sous le contrôle de la compagnie aérienne ou de son fournisseur de services (sous-traitant), sous une forme cryptée, les clés étant détenues par la compagnie aérienne ou son fournisseur de services, aux fins de l'identification?

2.3.2. si un tel traitement était jugé compatible, quelles garanties minimales appropriées seraient nécessaires, à la lumière des articles 25 et 32 du RGPD?

5. Après que l'autorité de contrôle française a estimé que le dossier était complet, le 16 février 2024, et que la présidente du comité l'a considéré comme complet le 23 février 2024, le secrétariat a diffusé le dossier le 23 février 2024. La présidente du comité a décidé, conformément à l'article 64, paragraphe 3, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur de l'EDPB, compte tenu de la complexité de la question, de prolonger de six semaines le délai par défaut de huit semaines.

### 1.2 Recevabilité de la demande d'avis en vertu de l'article 64, paragraphe 2, du RGPD

6. L'article 64, paragraphe 2, du RGPD prévoit, en particulier, que toute autorité de contrôle peut demander que toute question d'application générale ou produisant des effets dans plusieurs États membres soit examinée par le comité en vue d'obtenir un avis.

7. Le comité considère que la demande de l'autorité de contrôle française relative à la compatibilité de l'utilisation de la technologie de reconnaissance faciale pour l'authentification ou l'identification biométriques aux fins spécifiques de la rationalisation du flux de passagers dans les aéroports porte sur des questions «produisant des effets dans plusieurs États membres», car, comme expliqué dans la demande[5], plusieurs projets sont actuellement mis en œuvre dans les aéroports des États membres, et l'utilisation de cette technologie est appelée à s'intensifier dans les années à venir. Les modèles actuellement expérimentés par différents aéroports et compagnies aériennes variant considérablement d'un État membre à l'autre, il pourrait exister un risque qu'elle produise des effets divergents sur la protection des données dans plusieurs États membres.

8. Le comité estime par ailleurs que la demande soumise par l'autorité de contrôle française a des conséquences importantes pour l'application des principes énoncés à l'article 5, paragraphe 1, points e) et f), du RGPD, ainsi que pour les exigences applicables aux responsables du traitement en vertu de l'article 25 du RGPD, et les exigences applicables aux responsables du traitement et aux sous-traitants en vertu de l'article 32 du RGPD. Par conséquent, cette demande porte sur une «question d'application générale» au sens de l'article 64, paragraphe 2, du RGPD, puisqu'elle porte sur l'interprétation cohérente des principes de limitation de la conservation [article 5, paragraphe 1, point e), du RGPD] et d'intégrité et de confidentialité [article 5, paragraphe 1, point f), du RGPD], ainsi que sur les notions de protection des données dès la conception et de protection des données par défaut (article 25 du RGPD) et de sécurité des données (article 32 du RGPD) afin de garantir, entre autres, l'application cohérente de ces dispositions dans l'EEE.

9. Toute divergence éventuelle entre les États membres quant à l'interprétation de l'article 5, paragraphe 1, points e) et f), et des articles 25 et 32 du RGPD accroîtrait le risque que les exploitants d'aéroport et les compagnies aériennes développent des projets de reconnaissance faciale de manière

[5] Demande, p. 3.

non cohérente. Étant donné que l'autorité de contrôle française a démontré la nécessité manifeste d'une interprétation cohérente de ces dispositions en ce qui concerne la technologie de reconnaissance faciale pour l'authentification ou l'identification biométriques des passagers, dans le but de rationaliser le flux de passagers dans les aéroports[6], le comité estime que la demande est motivée, conformément à l'article 10, paragraphe 3, du règlement intérieur de l'EDPB.

10. Conformément à l'article 64, paragraphe 3, du RGPD, l'EDPB n'émet pas d'avis s'il a déjà émis un avis sur la même question[7]. L'EDPB n'a pas encore communiqué de réponses aux questions soulevées dans la demande. Bien que les lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo[8] fournissent déjà certains éléments utiles sur les mesures de sécurité qui devraient être appliquées au traitement des données biométriques, elles n'abordent pas tous les aspects des questions posées dans la demande. En outre, les lignes directrices publiées par l'EDPB, y compris les lignes directrices 3/2019 relatives aux dispositifs vidéo, ne fournissent pas d'indications spécifiques sur les éléments qui pourraient être vérifiés dans le cadre de la conservation centralisée ou décentralisée des données biométriques pour l'identification ou l'authentification des passagers dans le but de rationaliser le flux de passagers dans les aéroports, ni sur la compatibilité d'un tel traitement avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD.

11. Pour ces raisons, le comité estime que la demande est recevable et que les questions qui y sont soulevées devraient être analysées dans un avis adopté conformément à l'article 64, paragraphe 2, du RGPD.

## 2 CHAMP D'APPLICATION ET CONTEXTE DE L'AVIS

### 2.1 Champ d'application de l'avis

12. Le présent avis porte uniquement sur la compatibilité avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD de l'utilisation de la technologie de reconnaissance faciale pour l'authentification ou l'identification biométriques des passagers par les exploitants d'aéroport et les compagnies aériennes, **dans le but spécifique de rationaliser le flux de passagers dans les aéroports**, à savoir aux points de contrôle de sûreté, au point de collecte des bagages, à l'embarquement et à l'accès au salon des passagers, conformément à la demande.

13. En ce qui concerne le **champ d'application du présent avis**, le comité précise ce qui suit:

    1) le traitement des données à caractère personnel dans le cadre des contrôles aux frontières et les vérifications effectuées par les magasins hors taxes ne relèvent pas du champ d'application du présent avis, car ils sont réalisés par des responsables du traitement autres que des exploitants d'aéroport et des compagnies aériennes;

    2) l'utilisation de la technologie de reconnaissance faciale, même si elle est conforme aux scénarios décrits à la section 3.2 ci-dessous, à toute autre fin (telle que dans le

[6] Demande, p. 1 à 3.
[7] Article 64, paragraphe 3, du RGPD et article 10, paragraphe 4, du règlement intérieur de l'EDPB.
[8] Lignes directrices 3/2019 de l'EDPB sur le traitement des données à caractère personnel par des dispositifs vidéo, version 2.0, adoptées le 29 janvier 2020 (ci-après les «**lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo**»).

domaine répressif) ou par toute autre partie, même à des fins similaires, n'entre pas dans le champ d'application du présent avis;

3) le présent avis ne porte que sur le traitement des données à caractère personnel des passagers et ne couvre pas d'autres types de personnes concernées, tels que le personnel des exploitants d'aéroport ou des compagnies aériennes;

4) le présent avis examine la demande présentée par l'autorité de contrôle française en ce qui concerne la compatibilité des architectures de stockage des modèles biométriques des passagers avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD. À cet égard, il ne contient pas d'analyse complète et exhaustive du respect du RGPD par le ou les responsables du traitement concernés dans chaque cas, ainsi que par leur(s) sous-traitant(s), le cas échéant. Cela est particulièrement important compte tenu du fait que ces technologies présentent des risques accrus en ce qui concerne le traitement des catégories particulières de données au sens de l'article 9 du RGPD. Par conséquent, le présent avis est sans préjudice d'une évaluation de l'utilisation de technologies de reconnaissance faciale au regard d'autres dispositions du RGPD, notamment dans le secteur spécifique visé par la demande, ou d'une analyse juridique et technique au cas par cas fondée sur les circonstances propres à un responsable du traitement et le traitement spécifique envisagé par celui-ci;

5) le présent avis n'examine pas le traitement des données à caractère personnel des enfants et est sans préjudice de toutes exigences spécifiques s'appliquant à cet égard;

6) le présent avis est sans préjudice des exigences légales et restrictions supplémentaires concernant l'utilisation des données biométriques découlant des législations nationales des États membres[9];

7) toute conclusion formulée dans le présent avis est sans préjudice de nouvelles évolutions technologiques;

8) le présent avis examine quatre scénarios, dont les caractéristiques spécifiques sont décrites à la section 3.2 ci-après. Il n'examine pas d'autres scénarios, même si le traitement est effectué aux mêmes fins.

14. Dans sa demande, l'autorité de contrôle française a indiqué que le traitement des données biométriques des passagers dans le but de rationaliser le flux de passagers dans les aéroports serait fondé sur l'hypothèse que les passagers consentent à ce traitement, ce qui pourrait constituer la base juridique exigée par le RGPD[10]. **Toutefois, l'analyse de la base juridique applicable n'entre pas dans le champ d'application des questions soumises à l'EDPB dans la demande et, par conséquent, la validité du consentement pour un tel traitement conformément aux articles 6, 7 et 9 du RGPD n'est pas examinée dans le présent avis.**

[9] Par exemple, l'article 9, paragraphe 4, du RGPD prévoit que les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données biométriques.

[10] Demande, annexe I.

15. Néanmoins, l'EDPB observe, de manière générale, que, si les responsables du traitement concernés devaient s'appuyer sur cette base juridique, ils devraient obtenir un consentement explicite valable[11] de la part des personnes désireuses d'utiliser ces services. Ce consentement explicite devrait être libre, spécifique et éclairé[12], et la question de savoir si ces conditions sont remplies serait analysée au cas par cas. Cela signifie, notamment, que:

1) les personnes concernées devraient pouvoir retirer facilement ce consentement à tout moment et sans subir de préjudice[13];

2) pour que le consentement soit libre, une telle utilisation de technologies biométriques ne peut être mise en œuvre que sur une base volontaire, car les personnes devraient pouvoir choisir librement d'utiliser ou non ces services, sans subir de préjudice (tels que des délais nettement plus longs pour les passagers qui ne donnent pas leur consentement[14]) ou être exposées à des incitations, à des frais supplémentaires ou à l'offre d'avantages supplémentaires en contrepartie de leur consentement[15];

3) un consentement explicite devrait également être demandé aux personnes dont les données biométriques sont traitées, même si elles ne se sont pas inscrites pour être identifiées ou authentifiées par ces moyens. En d'autres termes, il est essentiel que les personnes qui n'ont pas explicitement consenti à la reconnaissance faciale aux fins prévues ne voient pas leur visage scanné par des caméras. À cette fin, il est possible, par exemple, de réserver certaines files d'attente à la reconnaissance faciale, en mettant en place une signalisation appropriée et une séparation physique des flux de contrôle non biométrique afin de permettre une identification claire de ces files;

4) sans préjudice de la question de savoir si le consentement constituerait la base juridique applicable pour un tel traitement, les principes de traitement consacrés à l'article 5 du RGPD en ce qui concerne la nécessité et la proportionnalité continuent de s'appliquer même lorsque les personnes ont donné leur consentement explicite à l'utilisation de leurs données biométriques[16].

---

[11] Selon l'article 4, paragraphe 14, et l'article 9, paragraphe 1, ainsi que l'article 9, paragraphe 2, point a), du RGPD, le traitement de données biométriques aux fins de l'identification d'une personne physique de manière unique est interdit, à moins que la personne concernée ait donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée à l'article 9, paragraphe 1, du RGPD, ne peut pas être levée par la personne concernée. Voir également les considérants 51, 52 et 53 du RGPD.

[12] Article 4, paragraphe 11, et article 7, du RGPD.

[13] Article 7, paragraphe 4, ainsi que considérant 50, du RGPD.

[14] Il pourrait s'agir, par exemple, de la conception d'un système visant à éviter de créer une pression sociale pesant sur les passagers qui ne souhaitent pas donner leur consentement, en faisant en sorte que le choix d'un passager n'ait pas de répercussion négative sur les autres passagers.

[15] Lignes directrices 05/2020 de l'EDPB sur le consentement au sens du règlement (UE) 2016/679, version 1.1, adoptées le 4 mai 2020 (ci-après les «**lignes directrices 5/2020 de l'EDPB sur le consentement**»), points 46 et 48.

[16] Idem, point 5.

16. L'autorité de contrôle française précise dans la demande[17] que les exploitants d'aéroport agiraient en qualité de responsables du traitement pour le traitement aux points de contrôle de sûreté de l'aéroport, tandis que les compagnies aériennes agiraient en qualité de responsables du traitement pour le traitement au point de collecte des bagages, à l'embarquement et à l'accès au salon des passagers. Le comité fait donc observer que différents acteurs pourraient intervenir dans le traitement décrit dans la demande et qu'il n'a pas évalué l'application des rôles de responsable du traitement (conjoint) et/ou de sous-traitant dans les scénarios décrits à la section 3.2 ci-dessous du présent avis. Dans chaque cas, les acteurs concernés doivent être identifiés et leurs responsabilités clairement définies, de façon à satisfaire aux exigences du RGPD[18].

17. En outre, le comité indique qu'à l'heure actuelle, il n'existe pas, dans l'Union européenne, d'obligation légale uniforme imposant aux exploitants d'aéroport et aux compagnies aériennes d'identifier les passagers et de vérifier que le nom figurant sur leur carte d'embarquement correspond au nom figurant sur leur document d'identité à tous les points de contrôle susmentionnés[19]. Ces exigences dépendent donc des législations nationales, qui peuvent varier d'un État membre à l'autre. Dans certains États membres, une telle vérification peut être requise à certains points de contrôle (par exemple, le point de collecte des bagages ou l'embarquement), tandis que dans d'autres, aucun contrôle de ce type n'est exigé actuellement[20]. L'existence d'obligations légales de vérifier l'identité des passagers a une incidence directe sur les pratiques des différents aéroports.

18. Par conséquent, dans ces situations, **lorsqu'aucun contrôle de l'identité des passagers au moyen d'un document d'identité officiel n'est requis, aucun contrôle ne devrait être effectué par des moyens biométriques, car cela constituerait un traitement excessif de données puisqu'un tel contrôle suppose le traitement de données supplémentaires par rapport à la situation actuelle et irait au-delà de ce qui est nécessaire à la finalité pertinente, en violation du principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), du RGPD.** Il convient de tenir compte de cette considération dans le cadre de l'examen de tous les scénarios décrits à la section 3.2 ci-dessous du présent avis.

### 2.2 Notions clés

[17] Demande, annexe I.

[18] Conformément à l'article 4, paragraphes 7 et 8, à l'article 5, paragraphe 2, et aux articles 24, 26, 28 et 29, du RGPD. Voir également les lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.1, adoptées le 7 juillet 2021.

[19] La réglementation pertinente au niveau de l'Union est le règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile. Toutefois, ce règlement ne traite pas du contrôle des documents d'identité officiels aux points de contrôle dans les aéroports, et les États membres ont toute latitude pour réglementer cette question au niveau national.

[20] Cela signifie qu'à l'heure actuelle, soit aucune vérification n'est effectuée, soit seule l'existence de la carte d'embarquement est vérifiée. Par exemple, selon le protocole du 22 mai 1954 exonérant les ressortissants du Danemark, de la Finlande, de la Norvège et de la Suède de l'obligation d'être munis d'un passeport ou d'un permis de séjour pour demeurer dans un pays nordique autre que le leur, à compter du 1er juillet 1954, les ressortissants de la Norvège, du Danemark, de la Finlande et de la Suède sont exonérés de l'obligation d'être munis d'un passeport ou d'un autre document d'identité de voyage lorsqu'ils voyagent entre ces pays.

19. Pour être qualifiées de données biométriques au sens de l'article 4, paragraphe 14, du RGPD[21], le traitement de données brutes, tels que des caractéristiques physiques, physiologiques ou comportementales d'une personne physique doit comprendre une mesure de ces caractéristiques, puisque les données biométriques sont obtenues au moyen de telles mesures[22].

20. À partir de l'image du visage d'une personne (photographie ou vidéo) appelée «**échantillon**» biométrique, il est possible d'extraire une représentation numérique de caractéristiques distinctes de ce visage (ce qui correspond à un «**modèle**»)[23]. En outre, le comité rappelle qu'«[u]n modèle biométrique est une représentation numérique des caractéristiques uniques qui ont été extraites d'un échantillon biométrique et qui peuvent être stockées dans une base de données biométriques»[24] qui permettent ou confirment l'identification d'une personne physique de manière unique. Par ailleurs, «[i]l est censé être unique et spécifique à chaque personne et il est, en principe, permanent dans le temps»[25]. Généralement, lors d'une comparaison visant à identifier ou à authentifier une personne au moyen de la reconnaissance faciale, un nouveau modèle biométrique est comparé à des objets stockés afin, soit de vérifier une correspondance, soit d'en trouver une dans une base de données[26].

21. La technologie de reconnaissance faciale peut remplir deux fonctions distinctes: l'authentification[27] et l'identification[28]. Bien que ces deux fonctions soient distinctes, elles reposent toutes deux sur le traitement de données biométriques relatives à une personne physique identifiée ou identifiable[29] et constituent de ce fait un traitement de catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD[30].

---

[21] Voir également les considérants 51, 52 et 53 du RGPD.

[22] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 74.

[23] Lignes directrices 05/2022 de l'EDPB sur l'utilisation de la technologie de reconnaissance faciale dans le domaine répressif, version 2.0, adoptées le 26 avril 2023 (ci-après les «**lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif**»), points 7 et 8.

[24] Idem, point 9.

[25] Idem.

[26] Lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif, points 10 et 11; voir également la norme internationale ISO/IEC 2382-37, 2022-03, disponible à l'adresse suivante: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [dernière consultation le 23 mai 2024] (ci-après la «**norme ISO/IEC 2382-37**»).

[27] Le comité fait observer que le futur règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) (non encore publié au Journal officiel), en son article 3, point 36), définit également la «vérification biométrique» comme suit: «vérification "un à un" automatisée, y compris l'authentification, de l'identité des personnes physiques en comparant leurs données biométriques à des données biométriques précédemment fournies» [voir la résolution législative du Parlement européen du 13 mars 2024 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union [COM(2021) 0206 – C9-0146/2021 – 2021/0106 (COD)].

[28] Idem; l'article 3, point 35), de la législation sur l'intelligence artificielle définit l'«identification biométrique» comme suit: «reconnaissance automatisée de caractéristiques physiques, physiologiques, comportementales ou psychologiques humaines aux fins d'établir l'identité d'une personne physique en comparant ses données biométriques à des données biométriques de personnes stockées dans une base de données».

[29] ISO/IEC 2382-37.

[30] Article 4, paragraphe 14, du RGPD, et lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif, point 12.

22. Concrètement:

l'**authentification** vise à confirmer une allégation biométrique par la comparaison. Il s'agit de la vérification en mode un à un;

l'**identification** vise à effectuer des recherches dans une base de données pour l'inscription des données biométriques afin de trouver des éléments d'identification attribuables à une seule personne. Il s'agit de l'identification en mode 1 à plusieurs.

23. Dans les deux cas (identification et authentification), les techniques de reconnaissance faciale reposent sur une estimation de la concordance entre les modèles, à savoir entre celui qui est comparé et le ou les modèles de référence. De ce point de vue, elles sont probabilistes: la comparaison déduit une probabilité plus ou moins élevée que la personne soit effectivement la personne à authentifier ou à identifier; si cette probabilité dépasse un certain seuil dans le système, défini par l'utilisateur ou le développeur du système, le système supposera l'existence d'une concordance[31].

[31] Lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif, point 11. Voir également ISO/IEC 2382-37.

## 3 SUR LE BIEN-FONDE DE LA DEMANDE

### 3.1 Observations générales

24. La présente section analyse les questions présentées au point 4 ci-dessus. Dans ce contexte, le comité analysera, pour la question 1, la compatibilité avec l'article 5, paragraphe 1, point f), et les articles 25 et 32 du RGPD, et, pour la question 2, la compatibilité avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD.

25. À cette fin, le comité analysera quatre scénarios différents[32], dont les caractéristiques spécifiques sont décrites à la section 3.2 ci-dessous.

26. À titre liminaire, le comité rappelle que l'utilisation de données biométriques, et de la technologie de reconnaissance faciale en particulier, présente des risques accrus pour les droits et libertés des personnes concernées. En premier lieu, le traitement en cause concerne des données biométriques qui bénéficient d'une protection spéciale en vertu de l'article 9 du RGPD. Notamment, les données biométriques changent de manière irrévocable la relation entre le corps et l'identité car elles rendent les caractéristiques physiques «lisibles par une machine» et sujettes à une utilisation ultérieure[33]. En outre, l'utilisation de la technologie de reconnaissance faciale peut comporter des risques liés aux faux négatifs, aux biais et à la discrimination[34], et la possibilité d'utilisation abusive des données biométriques pourrait avoir de graves conséquences pour les personnes, comme la fraude basée sur la ressemblance ou l'usurpation d'identité[35]. Il convient également de faire remarquer que, lorsque la reconnaissance faciale est effectuée à distance et sans la participation active de la personne concernée, celle-ci risque d'être encore moins consciente de ce traitement et des risques qui y sont associés. Enfin, il importe de souligner que les caractéristiques sur lesquelles sont fondées les données biométriques peuvent généralement être considérées comme permanentes et devraient être traitées comme irrévocables, en particulier dans le contexte de la reconnaissance faciale[36].

27. Par conséquent, compte tenu de ce qui précède, avant d'utiliser ces technologies, même si elles devaient être considérées comme particulièrement efficaces, les responsables du traitement

[32] Les quatre scénarios analysés par le comité sont fondés sur des cas d'utilisation présentés à l'annexe I de la demande. L'autorité de contrôle française a précisé que les cas d'utilisation présentés à l'annexe I de la demande étaient des exemples de mise en œuvre, relevant d'un scénario, utilisés à des fins d'illustration.
[33] Avis 3/2012 du groupe de travail «article 29» sur l'évolution des technologies biométriques, adopté le 27 avril 2012, WP193 (ci-après l'«**avis 3/2012 du groupe de travail "article 29" sur les technologies biométriques**»), p. 4. Il convient de noter que cet avis fait référence à la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après la «directive sur la protection des données»). Le RGPD a élargi le champ d'application des catégories particulières de données et, contrairement à la directive sur la protection des données, il considère que les données biométriques constituent des catégories particulières de données (article 9 du RGPD).
[34] Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Lignes directrices sur la reconnaissance faciale, juin 2021, p. 15; voir également les lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif, point 27.
[35] Avis 3/2012 du groupe de travail «article 29» sur les technologies biométriques, p. 29.
[36] Lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif, point 104.

devraient évaluer leur incidence sur les libertés et droits fondamentaux des personnes concernées et examiner si la finalité légitime du traitement peut être atteinte par des moyens moins intrusifs[37].

28. Le comité rappelle également que le droit à la protection des données à caractère personnel n'est pas un droit absolu et devrait être mis en balance avec d'autres droits fondamentaux protégés par la Charte conformément au principe de proportionnalité[38].

29. L'article 25, paragraphe 1, du RGPD fait référence aux «principes relatifs à la protection des données» qui sont énumérés à l'article 5 du RGPD[39] et exige de les mettre en œuvre dès la conception «de façon effective»[40]. Il inclut expressément le principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), du RGPD[41], qui exige que les données à caractère personnel soient «adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées et qui donne expression audit principe de proportionnalité»[42]. En outre, l'article 25, paragraphe 2, du RGPD précise l'obligation de «minimisation des données par défaut», en indiquant que cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation ainsi qu'à leur accessibilité[43].

30. Toutefois, l'article 25 du RGPD n'impose pas aux responsables du traitement de mettre en œuvre des mesures techniques et organisationnelles spécifiques, mais exige que les mesures et garanties choisies soient propres au contexte et aux risques que le traitement présente pour les droits et libertés de la

---

[37] Considérant 39 du RGPD. Voir également les lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 73.

[38] Considérant 4 du RGPD. Voir également, à cet égard, l'arrêt de la Cour du 22 juin 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504 (ci-après l'«arrêt dans l'affaire C-439/19, *Latvijas Republikas Saeima*»), points 98, 110 et 113. En outre, le principe de proportionnalité, qui fait partie des principes généraux du droit de l'Union, exige que les moyens mis en œuvre par un acte de l'Union soient aptes à réaliser l'objectif visé et n'aillent pas au-delà de ce qui est nécessaire pour l'atteindre [voir l'arrêt de la Cour du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, EU:C:2010:662 (ci-après l'«arrêt dans les affaires jointes C-92/09 et C-93/09, *Volker und Schecke*»), point 74 et jurisprudence citée].

[39] Lignes directrices 4/2019 de l'EDPB relatives à l'article 25 - Protection des données dès la conception et protection des données par défaut, version 2.0, adoptées le 20 octobre 2020 (ci-après les «**lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut**»), point 11.

[40] L'article 25, paragraphe 1, du RGPD dispose ce qui suit: «Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.» Voir également les lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 13.

[41] En conséquence, le considérant 39 du RGPD dispose que les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens.

[42] Arrêt dans l'affaire C-439/19, *Latvijas Republikas Saeima*, point 98; arrêt de la Cour du 11 décembre 2019, *Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064 (ci-après l'«arrêt dans l'affaire C-708/18, *M5A-ScaraA*»), point 48.

[43] Lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 48.

personne concernée[44]. De même, l'article 32 du RGPD relatif à la sécurité du traitement exige des responsables du traitement et des sous-traitants qu'ils mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les droits et libertés des personnes physiques.

31. Il importe de noter que, même si les passagers devaient consentir explicitement à l'utilisation de leurs données biométriques en vue de la rationalisation du flux de passagers dans les aéroports, les principes de traitement consacrés par le RGPD en ce qui concerne la nécessité et la proportionnalité s'appliquent toujours et doivent être respectés[45].

32. En ce qui concerne le **principe de nécessité**, le comité examinera si le traitement proposé est nécessaire pour atteindre l'objectif poursuivi et si le même objectif peut être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux libertés et droits fondamentaux de la personne concernée[46]. En ce qui concerne le **principe de proportionnalité**, le comité examinera si l'incidence négative sur les libertés et droits fondamentaux des personnes concernées est proportionnée à tout bénéfice escompté. Si le bénéfice est relativement mineur, cette incidence pourrait ne pas être proportionnée[47].

33. En tout état de cause, même si le comité considère que l'un des scénarios analysés ci-dessous pourrait satisfaire aux exigences de l'article 5, paragraphe 1, points e) et f), et des articles 25 et 32 du RGPD, il appartient au responsable du traitement, dans chaque cas, de le démontrer au moyen d'éléments factuels. Cette démonstration devrait inclure l'examen d'autres scénarios.

### 3.2 Sur la compatibilité avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD

#### 3.2.1 Scénario 1: conservation du modèle biométrique inscrit uniquement par la personne elle-même, aux fins de l'authentification

34. La présente section examine la compatibilité avec l'article 5, paragraphe 1, point f), et les articles 25 et 32 du RGPD de la conservation du modèle biométrique du passager uniquement par la personne elle-même, par exemple sur son appareil personnel[48], sous son contrôle exclusif[49], aux fins de l'authentification[50] (ci-après le «**scénario 1**»). Elle examine également les garanties appropriées pour le scénario 1, à la lumière des articles 25 et 32 du RGPD.

*Description du scénario*

[44] Lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 14.
[45] Lignes directrices 5/2020 de l'EDPB sur le consentement au sens du règlement (UE) 2016/679, point 5.
[46] Arrêt dans l'affaire C-439/19, *Latvijas Republikas Saeima*, points 110 et 113; et arrêt de la Cour (grande chambre) du 4 juillet 2023, *Meta/Bundeskartellamt*, C-252/21, EU:C:2023:537, point 108.
[47] Arrêts de la Cour dans les affaires C-708/18, *M5A-ScaraA*, points 52 à 56; C-92/09 et C-93/09, *Volker und Schecke*, point 87; et C-439/19, *Latvijas Republikas Saeima*, points 98, 110 et 113. Voir également l'avis 3/2012 du groupe de travail «article 29» sur les technologies biométriques, p. 8.
[48] La personne pourrait aussi imprimer et conserver son modèle biométrique sur papier.
[49] Cela est sans préjudice de la responsabilité globale du responsable du traitement à l'égard du traitement.
[50] Comme l'illustre le cas d'utilisation 1 présenté à l'annexe I de la demande.

35. Dans le scénario 1, le modèle biométrique inscrit de chaque passager, qui a consenti à ce traitement, est conservé par le seul passager, par exemple sur un appareil personnel qu'il détient, sous son contrôle exclusif. Les passagers sont authentifiés (comparaison un à un) lors de leur passage par des points de contrôle spécifiques de l'aéroport.

36. L'inscription est effectuée par l'exploitant de l'aéroport, soit à distance via son application[51], soit aux terminaux de l'aéroport avec un niveau approprié de garantie de l'identité (par exemple, le niveau de garantie approprié eIDAS[52]). Cette inscription consiste à enregistrer, sur l'appareil du passager, un modèle biométrique et les données d'identification[53] nécessaires au traitement. L'inscription n'a lieu qu'une seule fois et est valable pour une durée spécifique (par exemple, alignée sur la durée de validité du passeport des passagers). Ni les données d'identification des passagers, ni leurs données biométriques ne sont conservées par l'exploitant de l'aéroport après la procédure d'inscription.

37. En ce qui concerne la conservation en particulier, les données d'identification et le modèle biométrique des passagers sont conservés localement sur l'appareil de chaque passager (par exemple, sur l'application mobile de l'exploitant de l'aéroport ou sur une application de portefeuille numérique). L'appareil peut ensuite être utilisé pour transmettre ou interroger les données d'identification et le modèle biométrique des passagers, qui peuvent contenir des informations de vol et/ou la carte d'embarquement. Par exemple, ces informations sont cryptées au moyen d'une clé détenue par le seul exploitant de l'aéroport — éventuellement codée sous la forme d'un code QR, qui peut être imprimé sur papier ou affiché sur l'écran de l'appareil du passager. Dans ce cas, le passager présenterait ensuite ce code QR à des bornes de contrôle de l'aéroport spécialement prévues à cet effet et équipées d'un scanner QR et d'une caméra.

38. En ce qui concerne la sécurité, lors de l'établissement de correspondances, les codes QR sont décryptés au moyen d'une clé détenue par l'exploitant de l'aéroport, qui est le seul capable de décrypter lesdits codes. Les données biométriques des passagers ne sont conservées que pendant une très courte période et supprimées une fois les correspondances établies. Il convient d'observer que les mesures de sécurité en ce qui concerne la conservation dépendent en partie de la sécurité de l'appareil du passager.

*Évaluation de l'EDPB*

39. Le scénario 1 décrit les mesures techniques et organisationnelles destinées à garantir un niveau de sécurité adapté aux risques pour les personnes concernées, comme l'exigent l'article 5, paragraphe 1, point f), et l'article 32, du RGPD. Les passagers sont authentifiés (comparaison un à un) lors de leur passage par des points de contrôle spécifiques de l'aéroport. Dans ce scénario, la principale opération

[51] L'EDPB fait observer que d'autres modes d'inscription pourraient être envisagés à l'avenir et que l'inscription pourrait éventuellement être effectuée sans devoir recourir à l'application spécifique de l'exploitant de l'aéroport, par exemple au moyen d'une interaction avec le portefeuille numérique d'un utilisateur.

[52] Un cadre pour l'identification électronique et les services de confiance (ci-après «**eIDAS**») fondé sur le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique.

[53] Aux fins du présent avis, les données d'identification désignent les données, telles que le nom de famille, le prénom, la date de naissance, etc., dont l'exactitude a été vérifiée par rapport à un document d'identité ou un passeport.

d'établissement de correspondances est réalisée dans un environnement contrôlé[54], dans lequel les passagers participent activement au processus et ont davantage de contrôle sur leurs données. En particulier, seuls les passagers ayant consenti à un tel traitement seraient contrôlés et, étant donné que ce contrôle aurait lieu à des bornes spécialement prévues à cet effet, les données biométriques des autres passagers n'ayant pas consenti à un tel traitement ne seraient pas collectées. En outre, les passagers ayant donné leur consentement ont la possibilité de mettre un terme au traitement à tout moment en supprimant les données de leur appareil.

40. L'utilisation de la reconnaissance faciale sur la base d'un modèle biométrique conservé uniquement par la personne elle-même, qui peut, par exemple, se trouver sur un appareil personnel détenu par le passager, sous son contrôle exclusif, à des fins d'authentification à des points de contrôle spécifiques par l'intermédiaire d'une interface spécifique, présente, dans certaines conditions, moins de risques que l'utilisation de données biométriques lorsque les données sont stockées dans une base de données centralisée[55]. Ce stockage localisé, lorsqu'il est assorti de garanties appropriées[56], réduit la gravité des violations de données à caractère personnel par rapport au stockage centralisé, du point de vue du nombre de personnes concernées, et garantit que l'accès au modèle biométrique s'effectue avec la participation active de la personne concernée.

41. En outre, l'établissement de correspondances pourrait s'effectuer localement à l'aéroport, par la comparaison du modèle biométrique, par exemple inclus dans le code QR, avec le résultat du modèle calculé à partir de l'échantillon biométrique capté par la caméra de la borne de contrôle. Seul le résultat de l'établissement de correspondances serait connu du responsable du traitement effectuant un contrôle spécifique (qu'il s'agisse d'un exploitant d'aéroport ou d'une compagnie aérienne, selon que le contrôle est effectué aux points de contrôle de sûreté de l'aéroport, au point de collecte des bagages, à l'embarquement et/ou à l'accès au salon des passagers) et utilisé par ce dernier. De surcroît, le fait que les informations requises pour l'établissement de correspondances (par exemple, le code QR) doivent être fournies par la personne elle-même constitue un deuxième facteur[57] et renforce ainsi la sécurité de l'authentification.

42. En ce qui concerne la compatibilité avec l'article 25 du RGPD et, en particulier, afin de respecter l'exigence de minimisation des données, il convient de veiller à ce que le traitement respecte le principe de nécessité. Dans le scénario 1, les mesures choisies pourraient être considérées comme conformes au principe de nécessité au regard de l'objectif poursuivi (à savoir la rationalisation du flux de passagers) si, en fonction des circonstances du traitement, le responsable du traitement peut démontrer qu'il n'existe pas d'autres solutions moins intrusives qui permettraient d'atteindre le même objectif de manière aussi efficace. Par exemple, le responsable du traitement peut être en mesure de démontrer que, même si les passagers doivent montrer leur appareil, le scénario 1 accélère le processus de vérification par rapport à la situation actuelle, dans laquelle la vérification de la correspondance entre le nom inscrit sur la carte d'embarquement et celui figurant sur le document

[54] On entend par «environnement non contrôlé» l'utilisation de la reconnaissance faciale à des fins d'identification sans la participation active des personnes concernées, lorsque le modèle de chaque visage entrant dans la zone de surveillance est comparé aux modèles d'un large échantillon de la population stocké dans une base de données (voir lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif, point 17).

[55] Lignes directrices 5/2022 de l'EDPB sur la reconnaissance faciale dans le domaine répressif, point 17.

[56] Telles que décrites au point 46 ci-dessous.

[57] Par exemple, cela atténue le risque d'usurpation d'identité. Voir également la garantie C.1.2 ci-dessous.

d'identité du passager doit être effectuée par une personne[58]. À l'évidence, cela ne pourrait pas être démontré si, actuellement, aucun contrôle n'est effectué pour vérifier l'identité des passagers au moyen de leur document d'identité officiel (voir, à cet égard, le point 18 ci-dessus).

43. En outre, les modèles biométriques ne sont pas conservés par l'exploitant de l'aéroport après l'inscription, et la durée de conservation des données biométriques par le responsable du traitement qui procède au contrôle est très courte, puisque ces données sont effacées une fois les correspondances établies. Les mesures retenues dans le scénario 1 semblent donc limiter l'étendue du traitement et la durée de conservation des données à caractère personnel.

44. En ce qui concerne le principe de proportionnalité, le caractère intrusif d'un tel traitement peut être compensé par la participation active des passagers, car leurs données biométriques seraient conservées par eux seuls. En outre, compte tenu des mesures décrites ci-dessus et à supposer que le responsable du traitement mette en œuvre les garanties adéquates requises par le traitement spécifique en question, la mise en œuvre de mesures appropriées pourrait garantir un niveau de sécurité adapté au risque. Dans ce cas, l'incidence négative sur les libertés et droits fondamentaux des personnes concernées pourrait être considérée comme proportionnée au bénéfice escompté.

45. Par conséquent, compte tenu de ce qui précède, en réponse à la question 1.1, le comité conclut que ce traitement **pourrait être considéré comme étant, en principe, compatible avec l'article 5, paragraphe 1, point f), et les articles 25 et 32 du RGPD, sous réserve de garanties appropriées.**

*Garanties appropriées*

46. Dans ce type de scénario, en réponse à la question 1.2, l'EDPB estime qu'il convient de mettre en œuvre à tout le moins les garanties ci-après. D'autres garanties que celles décrites dans le présent avis pourraient être mises en œuvre pour atteindre les mêmes objectifs en matière de sécurité et de protection des données et être licites, pour autant qu'elles garantissent le respect du cadre juridique applicable.

47. Remarque: il s'agit d'un aperçu schématique non exhaustif des garanties appropriées possibles, qu'un responsable du traitement devrait mettre en œuvre dans une solution analogue au scénario 1. Leur caractère approprié au regard des articles 25 et 32 du RGPD dépendra d'une analyse au cas par cas. Tous les responsables du traitement devront veiller à réaliser leur propre analyse d'impact relative à la protection des données (ci-après «AIPD»)[59], et leurs solutions spécifiques peuvent nécessiter des mesures supplémentaires qui ne sont pas mentionnées dans le présent avis.

**A. Garanties générales**

**A.1 Analyse d'impact relative au traitement des données**

A.1.1 Procéder à une AIPD, conformément aux exigences de l'article 35 du RGPD, chaque fois que le responsable du traitement prévoit une nouvelle opération de traitement comportant un traitement susceptible d'engendrer un risque élevé. Tel est probablement le cas du

[58] On pourrait également faire valoir que le contrôle biométrique peut être moins sujet aux erreurs qu'un contrôle humain.
[59] Article 35 du RGPD.

scénario 1, car il suppose un traitement de données biométriques à grande échelle[60]. Évaluer le caractère approprié de la mise en œuvre d'un système de reconnaissance faciale, et notamment sa nécessité et sa proportionnalité au regard des objectifs poursuivis[61], au cours de la phase de conception initiale, et la réexaminer tout au long du cycle de développement du produit.

A.1.2 Consulter l'autorité de contrôle compétente si le traitement présente toujours un risque élevé en dépit des mesures prises par le responsable du traitement pour atténuer le risque[62].

**A.2 Droits conférés à la personne concernée et garanties pouvant être mises en œuvre par les responsables du traitement**

A.2.1 Garanties destinées à remédier aux faux négatifs. Atténuer le risque de biais liés à l'âge, au sexe et à la race en «[vérifiant] régulièrement si les algorithmes fonctionnent conformément aux finalités et adapter les algorithmes pour atténuer les biais constatés et garantir la loyauté du traitement»[63]. Par exemple, en mettant en œuvre une supervision et une intervention humaines, afin d'atténuer tout biais et de garantir l'absence de stigmatisation ou de profilage des passagers.

A.2.2 Veiller à ce que tous les traitements de données à caractère personnel soient transparents; à ce que les personnes soient informées de la manière dont leurs données sont traitées pour chaque opération de traitement et à ce qu'elles puissent exercer leur contrôle à cet égard[64].

A.2.3 Veiller à ce que des mesures soient mises en place pour respecter le principe de limitation des finalités afin que les données ne soient pas utilisées à d'autres fins, telles que la sécurité ou la formation.

A.2.4 Veiller à ne prendre aucune photo ou vidéo, même si elle n'est ni enregistrée ni traitée, de personnes qui ne consentent pas à la reconnaissance faciale en mettant en œuvre des mesures appropriées (par exemple, l'utilisation d'une profondeur de champ et d'une zone de capture adéquates afin d'éviter de capter des images d'autres passagers en arrière-plan ou alentour, la mise en place de files d'attente clairement désignées comme étant réservées à la reconnaissance faciale).

---

[60] Article 35, paragraphe 3, du RGPD, et lignes directrices du groupe de travail «article 29» concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, adoptées le 13 octobre 2017, WP248 rev.01, approuvées par l'EDPB.

[61] Article 35, paragraphe 7, point b), du RGPD.

[62] Article 36, paragraphe 1, du RGPD.

[63] Lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, note de bas de page 60, point 70.

[64] Lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 68, et considérant 7 du RGPD.

A.2.5 Lorsque les mêmes bornes peuvent être utilisées par les passagers qui consentent à la reconnaissance faciale et ceux qui n'y consentent pas, ou lorsque des passagers ne consentant pas à la reconnaissance faciale peuvent apparaître dans le champ visuel lorsque le système n'est pas utilisé, attendre une action positive de la part d'un passager consentant avant de commencer la capture d'une photo ou d'une vidéo.

A.2.6 Prévoir la possibilité pour une personne concernée de procéder à tout moment à l'effacement de données qu'elle est la seule à posséder (modèle biométrique[65]), détenues dans une application mobile ou un portefeuille numérique[66].

A.2.7 Prévoir des solutions de substitution ou des solutions de secours viables (c'est-à-dire pour les passagers qui ne consentiraient pas à l'utilisation de leurs données biométriques, pour les passagers qui ne seraient pas en mesure d'utiliser ces solutions, ou pour les passagers victimes de faux rejets), de manière à garantir également que les passagers qui ne consentent pas à l'utilisation de leurs données biométriques ne subissent aucun préjudice[67].

A.2.8 En cas d'utilisation d'une application, concevoir et configurer celle-ci de façon minutieuse afin de ne pas collecter de données inutiles et d'éviter l'utilisation de kits de développement logiciel tiers collectant des données à d'autres fins.

**A.3 Responsabilité**

A.3.1 Déterminer s'il existe des codes de conduite ou des mécanismes de certification pertinents pour aider à démontrer la conformité à la sécurité du traitement prévue à l'article 32 du RGPD[68]. Vérifier le caractère approprié des mesures pour le traitement spécifique en question. Les normes[69], les meilleures pratiques et les codes de conduite, qui sont reconnus par des associations et d'autres organismes représentant des catégories de responsables du traitement, peuvent être utiles pour déterminer les mesures appropriées.

A.3.2 Veiller à ce que des contrôles de sécurité de base soient effectués sur l'appareil des utilisateurs afin de permettre la phase d'inscription, même si le passager joue également un rôle dans la protection de ses données puisque celles-ci sont stockées sur son appareil. Des exemples de tels contrôles et vérifications techniques sont présentés dans la section C.2 «Infrastructure et réseau» ci-dessous.

**B. Garanties organisationnelles**

[65] Les références au modèle biométrique dans les garanties pour le scénario 1 correspondent aux références à la clé/au secret dans le scénario 2.
[66] Veuillez noter que cette garantie ne s'applique qu'au scénario 1.
[67] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 86.
[68] Article 32, paragraphe 3, du RGPD, et lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 10.
[69] Voir, par exemple, la norme ISO/IEC 2382-37.

**B.1 Politique et conformité**

B.1.1. Veiller à ce que des contrôles d'accès internes soient en place[70] et assortis de règles applicables aux administrateurs.

B.1.2 Lorsque le service de reconnaissance faciale peut être fourni par l'une des parties intervenant dans le traitement sans que les données d'identification ou les données biométriques, ou les deux, doivent être traitées par les autres parties impliquées, interdire que ces données transitent par ces autres parties. Par exemple, une compagnie aérienne n'a pas besoin d'accéder techniquement aux données biométriques lorsqu'elle utilise l'infrastructure commune de l'aéroport, même si elle agit en tant que responsable du traitement au sens du RGPD.

B.1.3 Définir une politique de cryptage et de gestion des clés[71], par exemple pour le traitement des données d'identification et des données biométriques.

B.1.4 Assurer la conformité avec le chapitre V du RGPD. Par exemple, garantir la conformité des transferts si, au cours de la procédure d'inscription, le responsable du traitement utilise un service à distance basé dans un pays tiers.

B.1.5 En cas de recours à des sous-traitants, veiller à ce qu'un contrat[72] soit établi, conformément à l'article 28, paragraphe 3, du RGPD.

B.1.6 Veiller à ce que des procédures soient en place pour gérer la supervision et l'intervention humaines, en particulier pour traiter les problèmes de faux rejets et les problèmes techniques ou de facilité d'utilisation.

**B.2 Formation et tests**

B.2.1. Veiller à ce que le personnel soit formé de manière appropriée.

B.2.2. Mettre en œuvre une «procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement»[73].

[70] Lignes directrices 4/2020 de l'EDPB relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19, adoptées le 21 avril 2020 (ci-après les «**lignes directrices 4/2020 de l'EDPB sur les données de localisation et les outils de recherche de contacts**»), SEC-10, p. 16.
[71] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 89.
[72] Article 28, paragraphe 3, du RGPD.
[73] Article 32, paragraphe 1, point d), du RGPD.

B.2.3. Mettre en œuvre un processus garantissant que le traitement du modèle biométrique[74] des passagers aux fins de l'authentification est techniquement efficace et suffisamment précis.

B.2.4. Veiller à ce que les échantillons biométriques collectés lors de l'inscription et au point de contrôle soient de qualité suffisante pour effectuer un traitement biométrique fiable.

**C. Garanties techniques**

**C.1 Accès**

C.1.1 Appliquer des garanties au cours de la phase d'inscription afin de veiller à démarrer le processus d'inscription avec une identité vérifiée. Par exemple, différentes étapes peuvent être mises en œuvre pour renforcer l'évaluation de l'authentification multifactorielle des identités des utilisateurs, qu'il s'agisse de liens uniques protégés par mot de passe pour activer l'application ou de mécanismes de déblocage des appareils locaux.

C.1.2 Appliquer des garanties pour remédier aux faux positifs, aux attaques par présentation et prévenir la fraude[75].

C.1.3 Interdire tout accès externe aux données d'identification et aux données biométriques[76].

C.1.4 Veiller à ce que le traitement soit effectué localement lors des phases d'inscription, de transmission et d'établissement de correspondances. Le point d'établissement de correspondances devrait être aussi proche que possible de l'appareil de la personne. Permettre la mise en correspondance du modèle sur l'appareil personnel pourrait nécessiter une interaction avec des prestataires de services situés en dehors de l'aéroport et l'utilisation de ressources du réseau public, ce qui aurait pour inconvénient de nuire à la disponibilité et de diffuser le modèle à des entités externes.

C.1.5 Authentifier un utilisateur pour l'ajout d'un nouveau vol et la création d'un nouveau code QR crypté.

C.1.6 Mettre en œuvre des mesures visant à remédier à la situation lorsqu'un passager perd l'accès à son code QR.

**C.2 Infrastructure et réseau**

C.2.1 Exiger le maintien à jour du système d'exploitation et l'activation de l'authentification donnant accès à l'appareil pour que l'application/le portefeuille numérique fonctionne, y

[74] Les références au modèle biométrique dans les garanties pour le scénario 1 correspondent aux références à la clé/au secret dans le scénario 2.
[75] Rapport de l'ENISA intitulé «Digital Identity: leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust» (Identité numérique: tirer parti du concept d'identité autonome pour renforcer la confiance), janvier 2022.
[76] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 89.

compris avec suppression automatique des données d'identification et des données biométriques si le système d'exploitation est obsolète et présente des risques de sécurité.

C.2.2 Isoler les unités d'établissement de correspondances (c'est-à-dire les bornes) du réseau lors de leur fonctionnement, et prendre toutes les autres mesures nécessaires pour assurer la sécurité.

C.2.3 Procéder à un établissement de correspondances biométriques sur l'appareil du passager ou sur la borne (traitement des données à la périphérie).

C.2.4 Prévoir des solutions pour remédier aux vulnérabilités en matière de sécurité des appareils personnels des passagers, notamment le cryptage (au minimum) des données biométriques et des données d'identification au repos.

C.2.5 Utiliser un stockage sécurisé pour (au moins) les données biométriques détenues par le seul utilisateur[77], par exemple en utilisant une enclave sécurisée (Secure Enclave) sur un smartphone.

C.2.6 Mettre en œuvre des garanties de sécurité afin de veiller à la sécurité physique des locaux, y compris le terminal biométrique de l'aéroport. Garantir un niveau élevé de sécurité pour les éléments de l'architecture qui traitent les données d'identification et les données biométriques (par exemple, le calcul, le flux de données, le stockage transitoire ou à long terme).

**C.3 Sécurité et gestion des données de contrôle d'identité de l'utilisateur**

C.3.1 Pendant la transmission et le stockage, compartimenter les données en au moins trois groupes différents, tels que: données d'identification, données biométriques et données de vol[78]. Veiller à ce que les données soient correctement cryptées entre la transmission et le stockage.

C.3.2 Mettre en place des mesures techniques visant à garantir que seules les données pouvant être traitées de manière licite à des points de contrôle spécifiques sont traitées et vérifiées au point de contrôle.

C.3.3 Veiller à l'efficacité de la suppression des données[79] en mettant en place une procédure de suppression sécurisée (par exemple, mémoire principale, cache, sauvegardes potentielles), et évaluer si la suppression des données doit être automatisée. Les durées de conservation

[77] Les références au modèle biométrique dans les garanties pour le scénario 1 correspondent aux références à la clé/au secret dans le scénario 2.
[78] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 89.
[79] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 89.

des données devraient être strictement appliquées au moyen de procédures automatiques, sans requérir une action supplémentaire de la part de la personne[80].

C.3.4 Garantir l'authenticité et l'intégrité des données (par exemple, la signature)[81].

C.3.5 Conserver les données biométriques des passagers au point d'inscription et au point de contrôle uniquement pour une durée très courte et les supprimer dès que le passager a passé le point de contrôle.

C.3.6 Si une application est utilisée pour l'inscription, appliquer les normes de sécurité applicables à la sécurité des applications mobiles lors du développement de l'application, ainsi que des tests de sécurité par un tiers.

C.3.7 Veiller à ce que la phase d'inscription à l'aéroport soit encadrée par des mesures de sécurité afin de préserver la confidentialité et l'intégrité des données biométriques des passagers. Par exemple, si le code QR est imprimé par la borne, il ne devrait pas y être affiché, afin d'éviter qu'un acteur malveillant ne le prenne en photo. En cas de transmission à courte portée, la transmission devrait s'effectuer avec la participation active de l'utilisateur et par un canal assurant la proximité.

C.3.8 Les données qui sont détenues uniquement par la personne elle-même[82] devraient être conservées dans un lieu de stockage sécurisé sur son appareil, et toute vulnérabilité possible liée aux systèmes d'exploitation de l'appareil doit être corrigée au moyen de correctifs de sécurité appropriés. Dans le cas d'un code QR imprimé, la personne devrait être informée du caractère particulièrement sensible des données qu'il contient et de ce qu'il permet d'effectuer.

C.3.9 Veiller à ce que l'inscription soit effectuée suivant des techniques adéquates de confirmation de l'identité à distance[83].

### 3.2.2 Scénario 2: stockage centralisé du modèle biométrique inscrit sous une forme cryptée au sein de l'aéroport, la clé/le secret étant détenu par le seul passager, aux fins de l'authentification

48. La présente section examine la compatibilité avec l'article 5, paragraphe 1, points e) et f), ainsi qu'avec les articles 25 et 32 du RGPD du stockage centralisé, aux fins de l'authentification, des modèles biométriques inscrits des passagers dans une base de données centralisée, sous une forme cryptée, la

[80] Lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 82.
[81] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 89.
[82] Les références au modèle biométrique dans les garanties pour le scénario 1 correspondent aux références à la clé/au secret dans le scénario 2.
[83] Voir le rapport de l'ENISA intitulé «Remote ID Proofing: Analysis of methods to carry out identity proofing remotely» (Confirmation de l'identité à distance: analyse des méthodes utilisées pour confirmer l'identité à distance), mars 2021.

clé/le secret étant détenu par le seul passager[84] (ci-après le «**scénario 2**»). Elle examine également les garanties appropriées pour le scénario 2, à la lumière des articles 25 et 32 du RGPD.

*Description du scénario*

49. Dans le scénario 2, l'inscription n'est effectuée qu'une seule fois, pour une durée de validité donnée (par exemple, un an après le dernier vol, et jusqu'à l'expiration de la validité du passeport), soit à distance au niveau approprié de garantie de l'identité (par exemple, le niveau de garantie approprié eIDAS), soit aux terminaux de l'aéroport. L'inscription est contrôlée par l'exploitant de l'aéroport et consiste à générer des données d'identification et des données biométriques qui sont cryptées au moyen d'une clé/d'un secret.

50. La base de données est stockée dans les locaux de l'aéroport, sous le contrôle de l'exploitant de l'aéroport. Les clés/secrets de cryptage spécifiques à la personne sont stockés uniquement sur l'appareil de celle-ci (par exemple, dans l'application mobile de l'exploitant de l'aéroport). L'application peut générer un code QR contenant la clé/le secret, qui peut, soit être imprimé sur papier, soit être affiché sur l'écran de l'appareil[85]. De surcroît, une seconde couche de cryptage est ajoutée[86] par l'exploitant de l'aéroport, au moyen de clés contrôlées par celui-ci.

51. Les passagers sont authentifiés (comparaison un à un) lors de leur passage par des points de contrôle spécifiques de l'aéroport. Les passagers qui choisissent de passer par les points de contrôle biométriques présentent leur code QR à une borne de contrôle spécialement prévue à cet effet et équipée d'un scanner QR et d'une caméra. L'index du passager est envoyé à la base de données pour demander le modèle crypté, qui est téléchargé et vérifié localement sur la borne et/ou l'appareil de l'utilisateur. Seul le résultat de l'établissement de correspondances est connu du responsable du traitement effectuant le contrôle au point de contrôle et utilisé par celui-ci[87].

52. Dans ce scénario, il n'y a pas de flux de données d'identification et de données biométriques entre les aéroports, ni d'interconnexion et d'interopérabilité entre les bases de données centralisées.

*Évaluation de l'EDPB*

53. Dans le scénario 2, les modèles biométriques inscrits des passagers sont stockés de manière centralisée, mais sous une forme cryptée, la clé/le secret étant détenu par les seuls passagers. Les passagers sont authentifiés (comparaison un à un).

54. Dans ce scénario, il est suggéré que l'objectif de rationalisation du flux de passagers (c'est-à-dire l'accélération des contrôles) pourrait être atteint grâce à l'utilisation d'un système centralisé. L'EDPB

[84] Comme l'illustre le cas d'utilisation 2 présenté à l'annexe I de la demande.
[85] L'autorité de contrôle française a précisé que d'autres solutions techniques pourraient également être envisagées pour envoyer les informations requises, par exemple l'utilisation d'un protocole de communication à courte portée.
[86] La clé/le secret (détenu par la personne) est lui-même crypté au moyen d'une autre clé détenue par l'exploitant de l'aéroport.
[87] L'autorité de contrôle française précise que cette durée de conservation est donnée à titre indicatif et peut être considérée comme acceptable étant donné que la clé est détenue par les personnes elles-mêmes et pourrait être choisie lors de la phase d'inscription. Il convient toutefois de faire observer que la durée de conservation peut être adaptée.

a fait observer précédemment qu'une telle solution pourrait être considérée comme une solution viable de substitution au stockage décentralisé des modèles biométriques inscrits[88] (tel que décrit dans le scénario 1), en présence de besoins objectifs et sous réserve de la mise en œuvre de garanties appropriées (voir garanties décrites à partir du point 60 ci-dessous).

55. En ce qui concerne les considérations de sécurité, les données de chaque personne sont cryptées au moyen de la clé spécifique détenue uniquement par la personne elle-même et sous son contrôle exclusif. En outre, le fait que les informations nécessaires à l'établissement de correspondances (c'est-à-dire la clé/le secret) doivent être fournies par la personne elle-même constitue un second facteur[89] et renforce ainsi la sécurité de l'authentification. De surcroît, une seconde couche de cryptage est ajoutée par l'exploitant de l'aéroport, au moyen de clés contrôlées par celui-ci. Dans le scénario 2, l'index de la personne est envoyé à la base de données centrale afin d'extraire les données biométriques qui lui sont associées. Ces données sont ensuite envoyées (cryptées) à un ordinateur situé au point de contrôle, où elles sont décryptées afin de procéder à l'établissement de correspondances, et seul le résultat de cette opération est connu du responsable du traitement effectuant le contrôle au point de contrôle et utilisé par celui-ci. À condition que la clé/le secret de la personne soit conservé dans l'ordinateur situé au point de contrôle et que seul l'index du passager soit envoyé à la base de données centrale afin d'extraire le modèle biométrique crypté, de telles mesures de sécurité pourraient donc être considérées comme compatibles avec l'article 5, paragraphe 1, point f), et l'article 32, du RGPD.

56. En ce qui concerne la compatibilité avec l'article 25 du RGPD, et en particulier afin de respecter l'exigence de minimisation des données, il convient de veiller à ce que le traitement respecte le principe de nécessité. Dans le scénario 2, les mesures choisies pourraient être considérées comme conformes au principe de nécessité au regard de l'objectif poursuivi (à savoir la rationalisation du flux de passagers dans les aéroports) si, en fonction des circonstances du traitement, le responsable du traitement peut démontrer qu'il n'existe pas d'autres solutions moins intrusives qui permettraient d'atteindre le même objectif de manière aussi efficace. Dans ce scénario, les passagers devraient toujours montrer leur appareil[90]. Néanmoins, le responsable du traitement peut être en mesure de démontrer que le scénario 2 accélère le processus de vérification par rapport à la situation actuelle, dans laquelle la vérification de la correspondance entre le nom inscrit sur la carte d'embarquement et celui figurant sur le document d'identité du passager doit être effectuée par une personne[91], ou par rapport au scénario 1. À l'évidence, cela ne pourrait pas être démontré si, actuellement, aucun contrôle n'est effectué pour vérifier l'identité des passagers au moyen de leur document d'identité officiel (voir, à cet égard, le point 18 ci-dessus).

57. En ce qui concerne le principe de proportionnalité, le caractère intrusif d'un tel traitement peut être compensé par la participation active des passagers, qui détiennent sous leur contrôle exclusif la clé d'accès à leurs données cryptées. Par ailleurs, il semble que les risques de sécurité liés au stockage

[88] Lignes directrices 3/2019 de l'EDPB relatives aux dispositifs vidéo, point 88.
[89] Par exemple, cela atténue le risque d'usurpation d'identité. Voir également la garantie C.1.2.
[90] L'autorité de contrôle française a également précisé qu'il pourrait aussi exister d'autres options pour présenter un modèle, par exemple une impression papier. En outre, l'EDPB reconnaît qu'à l'avenir, il pourrait être envisagé d'utiliser une autre technologie, par exemple une technologie fondée sur un système de communication en champ proche.
[91] On pourrait également faire valoir que le contrôle biométrique peut être moins sujet aux erreurs qu'un contrôle humain.

des données biométriques des passagers dans une base de données centralisée, lorsque la clé est détenue par les seuls passagers, puissent être atténués par la mise en œuvre de garanties appropriées (voir garanties décrites à partir du point 60 ci-dessous). Par conséquent, à supposer que le responsable du traitement mette en œuvre les garanties appropriées requises par le traitement spécifique en question, les risques pour les personnes pourraient être atténués et l'incidence négative sur les libertés et droits fondamentaux des personnes concernées pourrait être considérée comme proportionnée au bénéfice escompté. Bien entendu, dans chaque cas, il convient de veiller à ce que seules les données nécessaires à la finalité soient traitées et à ce que seuls les passagers ayant donné leur consentement soient contrôlés, de sorte qu'il n'existe aucun risque que les données biométriques d'autres passagers n'ayant pas donné leur consentement soient collectées.

58. Dans la demande, il est indiqué à titre d'exemple que, dans le scénario 2, la durée de conservation des données cryptées dans la base de données pourrait généralement être d'un an après le dernier vol effectué par la personne et aller jusqu'à l'expiration de la validité du passeport. Aucune information n'est fournie dans la demande pour justifier une durée aussi longue par des raisons objectives, bien qu'il puisse être présumé qu'une telle durée de conservation est envisagée à des fins de commodité pour des vols futurs. En ce qui concerne la durée de conservation, afin d'assurer la compatibilité avec l'article 5, paragraphe 1, point e), du RGPD dans ce scénario, les responsables du traitement devraient être en mesure de justifier la nécessité de cette durée de conservation par rapport à l'objectif visé dans des cas spécifiques. Le comité recommande aux responsables du traitement d'envisager la durée de conservation la plus courte possible, en tenant également compte des passagers qui ne prennent que très rarement l'avion, et de proposer aux personnes concernées de fixer la durée de conservation de leur choix.

59. À la lumière de ces considérations, en réponse à la question 2.1.1, le comité conclut que ce traitement **pourrait être considéré comme étant, en principe, compatible avec l'article 5, paragraphe 1, points e) et f), et les articles 25 et 32 du RGPD, sous réserve de garanties appropriées.**

*Garanties appropriées*

60. Dans ce type de scénario, en réponse à la question 2.1.2, le comité estime que, **outre les garanties énumérées dans le scénario 1**, il convient de mettre en œuvre à tout le moins les garanties ci-après. D'autres garanties que celles décrites dans le présent avis pourraient être mises en œuvre pour atteindre les mêmes objectifs en matière de sécurité et de protection des données et être licites, pour autant qu'elles garantissent le respect du cadre juridique applicable.

61. Remarque: *il s'agit d'un aperçu schématique non exhaustif des garanties appropriées possibles, qu'un responsable du traitement pourrait mettre en œuvre dans une solution analogue au scénario 2. Leur caractère approprié au regard des articles 25 et 32 du RGPD dépendra d'une analyse au cas par cas. Tous les responsables du traitement devront veiller à réaliser leur propre AIPD, et leurs solutions spécifiques peuvent nécessiter des mesures supplémentaires qui ne sont pas mentionnées dans le présent avis.*

## D. Garanties générales

### D.1 Droits conférés à la personne concernée et garanties pouvant être mises en œuvre par les responsables du traitement

D.1.1 Veiller à ce que le passager ait le contrôle des durées de conservation pour toutes ses données. Les durées de conservation devraient être limitées à ce qui est nécessaire à la finalité spécifique. Une durée maximale devrait être fixée au terme d'une analyse approfondie de facteurs tels que la validité du document d'identification. Les personnes concernées devraient se voir proposer de fixer la durée de conservation de leur choix, laquelle pourrait être plus courte que la durée de conservation par défaut.

D.1.2 Prévoir la possibilité pour une personne concernée de demander à tout moment l'effacement de données qu'elle est la seule à détenir (clé/secret), dans une application mobile ou un portefeuille numérique[92].

D.1.3 Veiller à ce que la localisation de la base de données centrale permette une surveillance effective par l'autorité de contrôle compétente.

## E. Garanties organisationnelles

### E.1 Politique et conformité

E.1.1 La confiance dans le serveur central doit être limitée. Veiller à ce que la gestion du serveur central suive des règles de gouvernance clairement définies et inclue toutes les mesures nécessaires pour garantir la sécurité dudit serveur[93].

## F. Garanties techniques

### F.1 Accès

F.1.1 Tenir des registres indiquant l'identité des personnes ayant accès aux données à caractère personnel, en particulier aux données d'identification et aux données biométriques, et le moment auquel ces données ont été consultées.

### F.2 Infrastructure et réseau

F.2.1 Sécuriser de façon appropriée la base de données centrale, notamment contre les attaques par déni de service.

F.2.2 Veiller à l'absence de connexion internet à la base de données centrale, aux bornes d'inscription et aux unités d'établissement de correspondances. L'exploitation et la maintenance de ce système (par exemple, sauvegarde, application de correctifs, surveillance, etc.) doivent s'effectuer localement, dans les locaux de l'aéroport.

### F.3 Sécurité et gestion des données

[92] Veuillez noter que cette garantie ne s'applique qu'au scénario 2.
[93] Lignes directrices 4/2020 de l'EDPB sur les données de localisation et les outils de recherche de contacts, PRIV-5, p. 17.

F.3.1 Mettre en œuvre des techniques cryptographiques de pointe pour sécuriser les échanges entre l'application et le serveur central[94].

F.3.2 Conserver la clé/le secret individuel au niveau où il sera utilisé pour décrypter (c'est-à-dire à la borne), et utiliser uniquement l'index pour récupérer le modèle biométrique inscrit correspondant dans la base de données centrale.

F.3.3 Veiller à ce que l'échange de clé/secret entre l'appareil de l'utilisateur et la borne protège la communication contre toute possibilité d'écoute ou de transmission à des tiers.

F.3.4 Indexer le modèle biométrique lorsqu'il est stocké dans la base de données centrale afin de permettre l'authentification en mode un à un, et veiller à ce qu'il soit unique et lié à la personne. Veiller à ce que l'index ne révèle aucune des informations d'identification du passager et ne soit pas corrélé à la clé de cryptage.

F.3.5 Authentifier et crypter de manière appropriée toute transmission entre la base de données centrale et les points de contrôle, et faire en sorte qu'elle ait lieu sur des réseaux isolés.

F.3.6 Éviter les liens bidirectionnels entre ensembles de données (données d'identification et données biométriques, ainsi que données de vol) et ne conserver que les liens unidirectionnels pertinents dans la base de données. Par exemple, ne conserver que les liens unidirectionnels de l'index vers les données d'identification, de l'index vers les données biométriques cryptées, et de l'index vers les données de vol.

F.3.7 Prévoir des dispositifs de continuité des activités, par exemple en mettant en place des systèmes de stockage de secours appropriés.

F.3.8 Veiller à ce que la borne ne conserve pas de registre des modèles cryptés ou non cryptés.

### 3.2.3 Stockage centralisé des modèles biométriques enregistrés aux fins de l'identification

62. La présente section examine la compatibilité avec l'article 5, paragraphe 1, points e) et f), ainsi qu'avec les articles 25 et 32 du RGPD du stockage centralisé, aux fins de l'identification, des modèles biométriques inscrits des passagers, lorsque ces modèles ne sont pas cryptés au moyen d'une clé/d'un secret détenu par le seul passager, dans deux cas d'utilisation: 1) lorsque ces modèles sont stockés

[94] Lignes directrices 4/2020 de l'EDPB sur les données de localisation et les outils de recherche de contacts, SEC-4, p. 19: «Parmi les techniques pouvant être utilisées figurent par exemple: le chiffrement symétrique et asymétrique, les fonctions de hachage, le test dit du "private membership", l'intersection d'ensemble privée, la récupération d'informations privées, le chiffrement homomorphique, etc.»

dans une base de données située au sein de l'aéroport, sous le contrôle de l'exploitant de l'aéroport[95] (ci-après le «**scénario 3.1**»), et 2) lorsque ces modèles sont stockés dans le nuage, sous le contrôle de la compagnie aérienne[96] (ci-après le «**scénario 3.2**»).

63. Le comité estime que l'utilisation de données biométriques à des fins d'**identification** dans de grandes bases de données centrales porte atteinte aux droits fondamentaux des personnes concernées et pourrait entraîner de graves conséquences pour ces dernières[97]. En outre, l'utilisation de données biométriques devrait également être examinée au regard de la finalité pour laquelle elles sont traitées, à la lumière des principes de nécessité et de proportionnalité[98].

#### *3.2.3.1 Scénario 3.1: stockage centralisé dans une base de données située au sein de l'aéroport, sous le contrôle de l'exploitant de l'aéroport*

*Description du scénario*

64. Dans le scénario 3.1, le modèle biométrique inscrit des passagers est stocké dans une base de données centrale située dans les locaux de l'aéroport et sous le contrôle de l'exploitant de l'aéroport, sous une forme cryptée. Plus précisément, les données des passagers sont compartimentées, ce qui signifie que leurs données d'identification, leur modèle biométrique inscrit et leurs données de vol sont stockées dans trois bases de données différentes. Ces données sont cryptées à l'aide de différentes clés, tant pendant le stockage que lors de leur transmission aux serveurs effectuant l'établissement de correspondances, où elles sont ensuite décryptées par l'exploitant de l'aéroport.

65. Les passagers doivent s'inscrire pour chaque vol, peu de temps avant leur départ (par exemple, 48 heures). Cette inscription peut s'effectuer soit à distance, soit aux terminaux des aéroports avec un niveau approprié de garantie d'identité (par exemple, le niveau de garantie approprié eIDAS). L'inscription peut également prendre la même forme que celle décrite dans le scénario 1, auquel cas les passagers doivent transférer leurs données de leur portefeuille numérique vers le système de l'aéroport dans les 48 heures précédant leur départ.

66. Dans ce scénario également, les passagers se présentent devant une borne de contrôle spécialement prévue à cet effet et équipée d'une caméra. Leur échantillon biométrique est ensuite envoyé à un serveur central de l'aéroport, qui recherchera des correspondances entre ces données et celles contenues dans la base de données biométriques centrale. Cela permet d'identifier le passager et de vérifier s'il est effectivement inscrit pour un vol au départ (ou pour le vol pour lequel l'embarquement est en cours en cas de contrôle à l'embarquement). Selon le point de contrôle, les données renvoyées au responsable du traitement du point de contrôle qui les demande peuvent être réduites à un minimum, par exemple à une réponse sous la forme «oui/non» ou au résultat de l'établissement de correspondances lui-même, si nécessaire. Dans ce cas, seul le résultat de la demande est transmis au responsable du traitement effectuant un contrôle au point de contrôle et utilisé par celui-ci.

---

[95] Comme l'illustre le cas d'utilisation 3A présenté à l'annexe I de la demande.
[96] Comme l'illustre le cas d'utilisation 3B présenté à l'annexe I de la demande.
[97] Voir, par exemple, l'avis 3/2012 du groupe de travail «article 29» sur les technologies biométriques, p. 8. Voir également le point 26 ci-dessus.
[98] Considérant 4 du RGPD. Voir également l'avis 3/2012 du groupe de travail «article 29» sur les technologies biométriques, p. 8.

67. Concrètement, dans ce scénario, les passagers sont identifiés au moyen d'une comparaison 1 à n, n étant le nombre de passagers attendus à l'aéroport sur une période de plusieurs jours. En outre, l'établissement de correspondances biométrique n'est effectué que lorsque les passagers se présentent à des points de contrôle prédéfinis à l'aéroport de départ, mais le traitement des données lui-même est effectué sur un serveur central relié à la base de données centrale. Dans ce scénario, la durée de conservation est généralement de 48 heures et les données sont effacées aussitôt après le décollage de l'avion.

*Évaluation de l'EDPB*

68. Comme rappelé ci-dessus, le traitement des données biométriques présente des risques accrus pour les droits et libertés des personnes concernées[99]. Ainsi, toute faille dans la sécurité des données peut entraîner des conséquences particulièrement graves pour les personnes concernées[100]. Les responsables du traitement sont tenus d'atténuer efficacement ces risques. Étant donné que, dans ce scénario, l'ensemble de l'architecture est totalement centralisé, le contrôle des passagers sur leurs données est plus limité. En outre, le risque que les données finissent par être traitées à d'autres fins que le contrôle du flux de passagers pourrait également être accru.

69. À la lumière du principe de sécurité et des exigences en la matière [article 5, paragraphe 1, point f), et article 32, du RGPD], il convient de considérer que le stockage des données d'identification et des données biométriques dans des bases de données centrales, bien que séparées, peut offrir des points d'attaque très utiles, et une violation de la confidentialité d'une telle base de données peut ensuite permettre d'accéder à l'ensemble des données. Ainsi, une éventuelle violation des modèles de reconnaissance faciale et des données d'identification qui y sont associées peut permettre l'identification non autorisée ou illicite des personnes concernées dans d'autres environnements. Elle peut également, selon les méthodes utilisées pour l'identification biométrique, menacer l'utilisation ultérieure de modèles de reconnaissance faciale en toute sécurité à des fins d'identification. Dans ce cas, les effets de la violation ne peuvent être atténués, contrairement à ce qui se passerait avec un autre type de justificatif (par exemple, nom d'utilisateur, mot de passe) pouvant être modifié[101].

70. En outre, la quantité et la qualité élevées des données d'identification et des données biométriques détenues par le responsable du traitement en font une cible de choix pour un attaquant, ce qui accroît le niveau de probabilité du risque de sécurité. Par ailleurs, les violations de données pourraient avoir des répercussions plus importantes car, du fait du stockage des données dans un lieu centralisé, les attaquants pourraient avoir plus facilement accès aux données à caractère personnel relatives à de nombreux passagers. Dès lors, une éventuelle violation pourrait exposer un grand nombre de personnes concernées à des risques particulièrement graves, par exemple l'usurpation d'identité à grande échelle, qui sont extrêmement difficiles à atténuer.

71. Par conséquent, en ce qui concerne la compatibilité avec l'article 5, paragraphe 1, point f), et l'article 32, du RGPD, les mesures envisagées dans le scénario 3.1[102], compte tenu de l'état de la technique, sont insuffisantes pour garantir un niveau de sécurité adapté au risque. Sur cette base, le

[99] Voir le point 26 ci-dessus.
[100] Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Lignes directrices sur la reconnaissance faciale, juin 2021, p. 22.
[101] Voir, à cet égard, l'avis 3/2012 du groupe de travail «article 29» sur les technologies biométriques, p. 37.
[102] Tel que décrit aux points 64 à 67 ci-dessus.

traitement envisagé dans le scénario 3.1 ne serait pas conforme à l'article 5, paragraphe 1, point f), et à l'article 32, du RGPD si un responsable du traitement se limitait à ces mesures.

72. À la lumière du principe énoncé à l'article 5, paragraphe 1, point e), du RGPD, dans ce scénario, la durée de conservation des données biométriques dans la base de données centrale est généralement de 48 heures. Une telle limitation de la conservation semble réduire considérablement les risques liés aux violations de données à caractère personnel. Néanmoins, la durée de conservation des données n'est pas un facteur déterminant en soi pour la compatibilité globale de ladite architecture, dès lors que ces durées de conservation peuvent être modifiées par les responsables du traitement. En tout état de cause, les mesures proposées doivent respecter les exigences de protection des données dès la conception et de protection des données par défaut énoncées à l'article 25 du RGPD.

73. Contrairement à ce qui est le cas dans les scénarios 1 et 2, dans lesquels les passagers sont authentifiés, dans le scénario 3.1, les passagers sont identifiés, au moyen d'une comparaison 1 à n, n étant le nombre de passagers attendus à l'aéroport sur une période de plusieurs jours qui ont consenti à ce traitement lors de leur passage par des points de contrôle spécifiques de l'aéroport. Cette identification suppose de rechercher des passagers dans une base de données centrale, en traitant chaque échantillon biométrique capturé afin de vérifier s'il correspond à une personne connue du système. Contrairement à ce qui est le cas dans le scénario 2, dans le scénario 3.1, les clés ne sont pas détenues par les seuls passagers. Par conséquent, dans ce scénario, les passagers ont beaucoup moins de contrôle sur leurs données biométriques. Le traitement proposé dans le scénario 3.1 ne saurait donc être compatible avec les exigences de protection des données dès la conception et de protection des données par défaut énoncées à l'article 25 du RGPD.

74. À la lumière de l'article 25 du RGPD, les responsables du traitement devraient tenir compte des types, des catégories et du niveau de détail des données à caractère personnel requises au regard des finalités du traitement[103]. Dans leurs choix de conception, les responsables du traitement devraient tenir compte des risques accrus que la collecte de quantités importantes de données à caractère personnel détaillées fait peser sur les principes d'intégrité et de confidentialité, de minimisation des données et de limitation de la conservation, et devraient comparer ces risques à la réduction des risques qu'entraîne la collecte d'informations moins détaillées et/ou en moins grande quantité au sujet des personnes concernées. En tout état de cause, le paramètre par défaut ne devrait pas inclure la collecte de données à caractère personnel qui ne sont pas nécessaires au regard de la finalité spécifique du traitement. En d'autres termes, si certaines catégories de données à caractère personnel ne sont pas nécessaires ou si des données détaillées ne sont pas requises car des données d'une granularité moins fine sont suffisantes, toute donnée à caractère personnel excédentaire ne devrait pas être collectée. Dans ce cas, si la mise en œuvre d'un autre traitement peut permettre d'atteindre le même objectif et est disponible selon les termes décrits dans le scénario 3.1, il n'est pas nécessaire d'utiliser la technologie de reconnaissance faciale.

75. En ce qui concerne l'article 25 du RGPD, un élément clé de la protection des données dès la conception et de la protection des données par défaut est l'autonomie de la personne concernée. En particulier, les personnes concernées devraient se voir accorder le degré d'autonomie le plus élevé possible pour déterminer l'utilisation qui est faite des données à caractère personnel les concernant, ainsi que la

[103] Lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 49.

portée et les conditions de cette utilisation ou de ce traitement[104]. Dans le scénario 1, la personne concernée disposerait d'une autonomie et d'un contrôle en ce qui concerne l'utilisation, la divulgation et l'effacement de ses modèles biométriques et, dans le scénario 2, elle conserverait un certain contrôle sur la divulgation de son propre modèle biométrique, puisqu'elle détiendrait elle-même la clé de cryptage/le secret. En revanche, dans le scénario 3.1, la personne concernée est totalement dépendante des choix du responsable du traitement en ce qui concerne le traitement de ses données biométriques et n'a donc pas de contrôle direct sur l'utilisation de son modèle biométrique.

76. En ce qui concerne la compatibilité avec l'article 25 du RGPD, et en particulier pour respecter l'exigence de minimisation des données, le traitement envisagé dans le scénario 3.1 ne peut satisfaire au principe de nécessité. Le comité estime qu'un résultat similaire pour rationaliser le flux de passagers dans les aéroports peut être obtenu d'une manière moins attentatoire à la vie privée. Par exemple, cet objectif peut être atteint sans l'utilisation de données biométriques (même si l'expérience de l'utilisateur serait alors différente, car le processus de présentation de la carte d'embarquement et, le cas échéant, de documents d'identification officiels pourrait être plus long). En outre, d'autres solutions, notamment celles qui reposent sur le stockage des données biométriques dans un portefeuille local sur l'appareil de la personne ou celles nécessitant le cryptage des données au moyen d'une clé spécifique stockée dans l'appareil de la personne, permettent d'atteindre les objectifs d'une manière moins attentatoire à la vie privée.

77. En ce qui concerne le principe de proportionnalité, le traitement envisagé dans le scénario 3.1 présenterait, pour les droits des personnes concernées, des risques qui ne seraient pas atténués par les garanties envisagées compte tenu de l'état actuel de la technique. Le risque d'incidence négative sur les libertés et droits fondamentaux des personnes concernées qui pourrait résulter d'une violation de données dans une base de données centralisée renfermant les données biométriques d'un grand nombre de personnes semble l'emporter sur le bénéfice escompté du traitement, étant donné que ce bénéfice, à savoir une légère facilitation et accélération des contrôles, est relativement mineur. Par conséquent, il ne saurait justifier le caractère intrusif élevé de ces mesures pour les libertés et droits fondamentaux des personnes, et le traitement envisagé dans le scénario 3.1 ne satisfait pas au principe de proportionnalité.

78. À la lumière de ces considérations, en réponse à la question 2.2.1, le comité conclut que, lorsque le traitement est effectué dans le but spécifique de rationaliser le flux de passagers dans les aéroports, le traitement envisagé dans le scénario 3.1:

- **ne saurait être compatible avec l'article 25 du RGPD**;
- **ne serait pas conforme à l'article 5, paragraphe 1, point f), et à l'article 32, du RGPD** si un responsable du traitement se limitait aux mesures décrites dans ce scénario.

[104] Lignes directrices 4/2019 de l'EDPB sur la protection des données dès la conception et la protection des données par défaut, point 70. Le considérant 7 du RGPD précise en outre que «[l]es personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant».

#### *3.2.3.2 Scénario 3.2: stockage centralisé dans un nuage, sous le contrôle de la compagnie aérienne*

*Description du scénario*

79. Dans le scénario 3.2, le modèle biométrique inscrit des passagers est stocké dans le nuage, sous le contrôle de la compagnie aérienne ou de son fournisseur de services en nuage (sous-traitant). Dans la demande, il est précisé que le fournisseur de services en nuage serait situé dans l'EEE[105]. Dans ce cas, les données des passagers sont cryptées, mais décryptées lorsqu'elles sont utilisées (par exemple, lors de l'opération d'établissement de correspondances), et les clés sont sous le contrôle de la compagnie aérienne ou de son fournisseur de services en nuage. Les données biométriques des passagers sont utilisées aux fins de l'identification des passagers au moyen d'une comparaison 1 à n, n pouvant atteindre le nombre total de clients de la compagnie aérienne[106].

80. Comme dans les scénarios 1, 2 et 3.1, dans ce cas également, les passagers doivent d'abord s'inscrire. Toutefois, dans le scénario 3.2, leur inscription s'effectue une seule fois, pour toute la durée pendant laquelle le client détient un compte auprès de la compagnie aérienne. L'inscription s'effectue soit à distance à un niveau approprié de garantie de l'identité (par exemple, le niveau de garantie approprié eIDAS) soit aux terminaux de l'aéroport. L'établissement de correspondances biométrique n'est effectué que lorsque les passagers se présentent à des points de contrôle prédéfinis dans l'aéroport, mais le traitement des données en lui-même est effectué dans le nuage.

81. À l'aéroport, les passagers passent par des bornes de contrôle spécialement prévues à cet effet et équipées d'une caméra. Leurs données biométriques sont envoyées par l'intermédiaire d'une demande au serveur en nuage d'une compagnie aérienne, où des correspondances avec ces données sont recherchées dans la base de données centrale. Cela permet d'identifier le passager et de vérifier s'il est effectivement inscrit pour un vol au départ (ou pour le vol pour lequel l'embarquement est en cours en cas de contrôle à l'embarquement).

82. Les résultats de l'établissement de correspondances peuvent être mis à la disposition de plusieurs exploitants d'aéroport lorsqu'une compagnie aérienne y dispose d'un terminal spécifique à cet effet ou d'un accès à l'infrastructure du système d'information commun d'un aéroport. Selon le point de contrôle, les données renvoyées au responsable du traitement du point de contrôle qui les demande peuvent être réduites à un minimum, par exemple à une réponse sous la forme «oui/non» ou au résultat de l'établissement de correspondances lui-même, si nécessaire. Dans ce cas, seul le résultat de la demande est connu du responsable du traitement effectuant un contrôle au point de contrôle et utilisé par celui-ci.

83. La durée de conservation du modèle est définie par la compagnie aérienne et peut être alignée sur la durée pendant laquelle le client détient un compte auprès de la compagnie aérienne.

*Évaluation de l'EDPB*

[105] L'autorité de contrôle française a précisé qu'il s'agissait là d'un exemple et que les fournisseurs de services en nuage qui ne sont pas établis dans l'EEE pourraient également être envisagés. En outre, d'autres solutions de stockage (par exemple, sans utilisation du nuage) pourraient également être envisagées.
[106] L'autorité de contrôle française a précisé qu'il s'agissait d'un exemple, et qu'il existe une solution dans laquelle les données biométriques sont chaque fois transmises en mode «push» avant le vol.

84. Les considérations déjà exprimées par le comité en ce qui concerne le scénario 3.1[107] s'appliquent également au présent scénario.

85. En ce qui concerne le principe de sécurité et les exigences en la matière [article 5, paragraphe 1, point f), et article 32 du RGPD], dans le scénario 3.2, le traitement s'effectue dans le nuage et de nombreuses entités pourraient avoir accès aux données, y compris potentiellement des fournisseurs établis en dehors de l'EEE, même lorsque les données sont détenues dans l'EEE[108]. Une telle architecture peut comporter des risques en ce qui concerne les transferts de données à caractère personnel vers des pays tiers. En outre, bien que les données des passagers soient cryptées, elles sont décryptées lorsqu'elles sont utilisées (par exemple, lors de l'opération d'établissement de correspondances), et les clés sont sous le contrôle de la compagnie aérienne ou de son fournisseur de services en nuage. Un tel stockage peut avoir pour effet d'accroître davantage l'exposition aux risques de sécurité.

86. Par conséquent, en ce qui concerne la compatibilité avec l'article 5, paragraphe 1, point f), et l'article 32, du RGPD, les mesures envisagées dans le scénario 3.2[109], compte tenu de l'état de la technique, sont insuffisantes pour garantir un niveau de sécurité adapté au risque. Sur cette base, le traitement envisagé dans le scénario 3.2 ne serait pas conforme à l'article 5, paragraphe 1, point f), et à l'article 32, du RGPD si un responsable du traitement se limitait à ces mesures.

87. Par ailleurs, selon le scénario 3.2[110], les données pourraient être conservées pendant une durée significative (c'est-à-dire, potentiellement, aussi longtemps que la personne concernée détient un compte auprès de la compagnie aérienne). Une telle durée de conservation expose les données à un risque accru de violation de leur confidentialité et de leur intégrité, et semble aller au-delà de ce qui est strictement nécessaire et proportionné aux fins du traitement. Le comité fait observer que la durée de conservation des données n'est pas un facteur déterminant en soi pour la compatibilité globale de ladite architecture avec le RGPD, dès lors qu'elle est susceptible d'être modifiée par les responsables du traitement. Toutefois, sur la base des informations dont il dispose et qui figurent dans la description du scénario 3.2, cette longue durée de conservation n'est pas suffisamment justifiée et aucune mesure ne semble être prise pour atténuer les risques pour les personnes. De ce fait, la durée de conservation proposée ne serait pas limitée à ce qui est nécessaire, comme l'exige le principe de limitation de la conservation prévu à l'article 5, paragraphe 1, point e), du RGPD.

88. En tout état de cause, les mesures proposées dans le scénario 3.2 ne sauraient satisfaire aux exigences de protection des données dès la conception et de protection des données par défaut prévues à l'article 25 du RGPD. Dans ce scénario, les modèles biométriques inscrits des passagers sont stockés dans le nuage, sous le contrôle de la compagnie aérienne ou de son fournisseur de services en nuage (sous-traitant). Comme expliqué ci-dessus, de nombreuses entités pourraient avoir accès à ces données. En outre, les données biométriques des passagers sont utilisées aux fins de l'identification des passagers par une comparaison 1 à n, n pouvant aller jusqu'au nombre total d'utilisateurs/de clients de la compagnie aérienne. Cette méthode consiste à trouver une personne parmi un groupe

[107] Points 68 à 77 ci-dessus.
[108] EDPB, *2022 Coordinated Enforcement Action on the use of Cloud-based services by the public sector* (Action d'application coordonnée sur l'utilisation des services en nuage par le secteur public), 17 janvier 2023, p. 19.
[109] Voir points 79 à 83 ci-dessus.
[110] Voir point 83 ci-dessus.

de personnes figurant dans la base de données centrale, en traitant chaque visage capturé afin de vérifier s'il correspond à une personne connue du système. Contrairement à ce qui est le cas dans le scénario 3.1, dans le scénario 3.2, la comparaison pourrait être effectuée à une échelle beaucoup plus large, étant donné que le critère, dans ce cas précis, est le nombre total de clients de la compagnie aérienne, tandis que, dans le scénario 3.1, seul le nombre de passagers attendus sur une période de plusieurs jours est pris en considération.

89. En outre, en ce qui concerne la compatibilité avec l'article 25 du RGPD, et en particulier pour respecter l'exigence de minimisation des données, le traitement envisagé dans le scénario 3.2 ne peut satisfaire au principe de nécessité. Le comité estime qu'un résultat similaire pour rationaliser le flux de passagers dans les aéroports pourrait être obtenu par d'autres mesures moins intrusives, par exemple sans l'utilisation de données biométriques, même si l'expérience de l'utilisateur serait alors différente, car le processus de présentation des documents d'identité et de la carte d'embarquement pourrait être plus long. De surcroît, d'autres solutions, notamment celles qui reposent sur le stockage des données biométriques dans un portefeuille local sur l'appareil de la personne ou celles nécessitant le cryptage des données au moyen d'une clé spécifique stockée dans l'appareil de la personne, permettent au responsable du traitement d'atteindre les objectifs d'une manière moins attentatoire à la vie privée.

90. En ce qui concerne le principe de proportionnalité, le traitement envisagé dans le scénario 3.2 présenterait, pour les droits des personnes concernées, des risques qui ne seraient pas atténués par les garanties envisagées. L'incidence négative sur les libertés et droits fondamentaux des personnes concernées qui résulterait d'une violation de données dans une base de données centralisée renfermant les données biométriques d'un grand nombre de personnes stockées dans le nuage semble l'emporter sur le bénéfice escompté du traitement, étant donné que ce bénéfice, à savoir une légère facilitation et accélération des contrôles, est relativement mineur. Par conséquent, il ne saurait justifier le caractère intrusif élevé de ces mesures pour les libertés et droits fondamentaux des personnes, et le traitement envisagé dans le scénario 3.2 ne saurait être considéré comme proportionné.

91. À la lumière de ces considérations, en réponse à la question 2.3.1, le comité conclut que, lorsque le traitement est effectué dans le but spécifique de rationaliser le flux de passagers dans les aéroports, le traitement envisagé dans le scénario 3.2:

- **ne saurait être compatible avec l'article 25 du RGPD**;
- **ne serait pas conforme à l'article 5, paragraphe 1, point f), et à l'article 32, du RGPD** si un responsable du traitement se limitait aux mesures décrites dans ce scénario;
- **ne serait pas conforme à l'article 5, paragraphe 1, point e), du RGPD,** étant donné que, sur la base des informations dont dispose le comité, la durée de conservation envisagée dans le scénario 3.2 n'est pas suffisamment justifiée. Pour respecter le principe de limitation de la conservation énoncé à l'article 5, paragraphe 1, point e), du RGPD, le responsable du traitement devrait démontrer que les données à caractère personnel ne sont pas conservées plus longtemps que ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

## 4 CONCLUSIONS

92. En ce qui concerne la question 1.1, sur la base de la demande d'avis de l'autorité de contrôle française, en ce qui concerne les exigences de l'article 5, paragraphe 1, point f), et des articles 25 et 32 du RGPD, et sur la base de l'analyse qui précède, le comité conclut ce qui suit:

93. l'utilisation de la technologie de reconnaissance faciale à des fins d'authentification biométrique, dans le but spécifique de rationaliser le flux de passagers dans les aéroports (points de contrôle de sûreté, point de collecte des bagages, embarquement et accès au salon des passagers) pourrait être considérée comme étant, en principe, compatible avec les principes d'intégrité et de confidentialité énoncés à l'article 5, paragraphe 1, point f), et aux articles 25 et 32 du RGPD, dans le cas d'une architecture de stockage dans laquelle le modèle biométrique inscrit de chaque passager est stocké localement sur leur appareil personnel et sous leur contrôle exclusif, sous réserve des garanties appropriées décrites au point 46 ci-dessus.

94. En ce qui concerne la question 2.1.1, sur la base de la demande d'avis de l'autorité de contrôle française, en ce qui concerne les exigences de l'article 5, paragraphe 1, points e) et f), et des articles 25 et 32 du RGPD, et sur la base de l'analyse qui précède, le comité conclut ce qui suit:

95. l'utilisation de la technologie de reconnaissance faciale à des fins d'authentification biométrique, dans le but spécifique de rationaliser le flux de passagers dans les aéroports (points de contrôle de sûreté, point de collecte des bagages, embarquement et accès au salon des passagers) pourrait être considérée comme étant, en principe, compatible avec le principe de limitation de la conservation prévu à l'article 5, paragraphe 1, point e), et avec les principes d'intégrité et de confidentialité énoncés à l'article 5, paragraphe 1, point f), et aux articles 25 et 32 du RGPD dans le cas d'une architecture de stockage centralisée, dans laquelle le modèle biométrique inscrit de chaque passager est stocké dans une base de données centrale située au sein de l'aéroport, sous le contrôle de l'exploitant de l'aéroport, sous une forme cryptée, la clé/le secret étant détenu uniquement par la personne elle-même, sous réserve des garanties appropriées telles que décrites à partir du point 60 ci-dessus.

96. En ce qui concerne la question 2.2.1, sur la base de la demande d'avis de l'autorité de contrôle française en ce qui concerne les exigences de l'article 5, paragraphe 1, points e) et f), et des articles 25 et 32 du RGPD et sur la base de l'analyse qui précède, le comité conclut ce qui suit:

97. l'utilisation de la technologie de reconnaissance faciale à des fins d'authentification biométrique, dans le but spécifique de rationaliser le flux de passagers dans les aéroports (points de contrôle de sûreté, point de collecte des bagages, embarquement et accès au salon des passagers), dans le cas d'une architecture de stockage centralisée dans laquelle les modèles biométriques inscrits des passagers ne sont pas cryptés au moyen d'une clé/d'un secret détenu par le seul passager, et dans laquelle ces modèles sont stockés dans une base de données située au sein de l'aéroport (sous le contrôle de l'exploitant de l'aéroport), ne saurait être compatible avec l'article 25 du RGPD. En outre, un tel traitement ne serait pas conforme aux principes d'intégrité et de confidentialité énoncés à l'article 5, paragraphe 1, point f), et à l'article 32, du RGPD, si un responsable du traitement se limitait aux mesures décrites dans le scénario 3.1.

98. En ce qui concerne la question 2.3.1, sur la base de la demande d'avis de l'autorité de contrôle française en ce qui concerne les exigences de l'article 5, paragraphe 1, points e) et f), et des articles 25 et 32 du RGPD et sur la base de l'analyse qui précède, le comité conclut ce qui suit:

99. l'utilisation de la technologie de reconnaissance faciale à des fins d'authentification biométrique, dans le but spécifique de rationaliser le flux de passagers dans les aéroports (points de contrôle de sûreté,

point de collecte des bagages, embarquement et accès au salon des passagers), dans le cas d'une architecture de stockage centralisée dans laquelle les modèles biométriques inscrits des passagers ne sont pas cryptés au moyen d'une clé/d'un secret détenu par le seul passager, et dans laquelle ces modèles sont stockés dans le nuage (sous le contrôle de la compagnie aérienne), ne saurait être compatible avec l'article 25 du RGPD. En outre, un tel traitement ne serait pas conforme aux principes d'intégrité et de confidentialité énoncés à l'article 5, paragraphe 1, point f), et à l'article 32, du RGPD, si un responsable du traitement se limitait aux mesures décrites dans le scénario 3.2. Enfin, sur la base de la description du scénario 3.2 et des informations dont dispose le comité, le traitement ne serait pas conforme au principe de limitation de la conservation énoncé à l'article 5, paragraphe 1, point e), du RGPD.

Pour le Comité européen de la protection des données

La présidente

(Anu Talus)