

Opinion of the Board (Art. 64)



**Dictamen 11/2024 sobre el uso del reconocimiento facial
para agilizar el flujo de pasajeros en aeropuertos
(compatibilidad con los artículos 5, apartado 1, letras e) y f), y
25 y 32 del RGPD**

Versión 1.1

Adoptado el 23 de mayo de 2024

TRADUCCIÓN NO OFICIAL

Resumen ejecutivo

La Autoridad de Control francesa solicitó al Comité Europeo de Protección de Datos que emitiera un dictamen sobre el uso de la tecnología de reconocimiento facial por parte de los operadores aeroportuarios y las compañías aéreas para la autenticación o identificación biométrica de los pasajeros con el fin de agilizar el flujo de pasajeros en los aeropuertos.

Como observación preliminar, el Comité recuerda que el uso de datos biométricos y, en particular, de la tecnología de reconocimiento facial entraña un muy alto riesgo para los derechos y libertades de los interesados. Esta supone el tratamiento de datos biométricos, los cuales están sometidos a un régimen de especial protección en virtud del artículo 9 del RGPD. Antes de utilizar dichas tecnologías, incluso si se consideraran especialmente eficaces, los responsables del tratamiento deben evaluar el impacto en los derechos y libertades fundamentales de los interesados y considerar si medios menos intrusivos pueden lograr el objetivo legítimo del tratamiento.

El alcance de este Dictamen, según la solicitud, se limita a la compatibilidad del tratamiento con el **artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD** con el **fin específico de racionalizar el flujo de pasajeros en los aeropuertos** en cuatro puntos de control específicos: los controles de seguridad, la entrega de equipaje, el embarque y el acceso a la sala de pasajeros (N.T.: Salas VIP de los aeropuertos). El presente Dictamen no incluye un análisis completo y exhaustivo sobre el cumplimiento del RGPD por parte del responsable o responsables del tratamiento pertinentes en cada caso, así como de su(s) encargado(s), en su caso. Por lo tanto, el presente dictamen se entiende sin perjuicio de un análisis jurídico y técnico caso por caso basado en el tratamiento y las circunstancias específicas previstas por el responsable del tratamiento. Además, el análisis de la base jurídica aplicable no entra en el ámbito de las cuestiones planteadas al Comité en la solicitud y, en consecuencia, la validez del consentimiento para dicho tratamiento, de conformidad con los artículos 6, 7 y 9 del RGPD, no se examina en las presentes conclusiones. Además, el presente dictamen se entiende sin perjuicio de las restricciones al uso de datos biométricos establecidas en la legislación de los Estados miembros.

En este dictamen, el Comité evalúa la conformidad del tratamiento con las disposiciones del RGPD mencionadas anteriormente en el contexto de **cuatro escenarios específicos**.

El **primer escenario** implica el almacenamiento de una plantilla biométrica en manos de la persona interesada, por ejemplo, en su dispositivo individual, bajo su control exclusivo para autenticar (comparación 1:1) el pasajero a medida que avanza a través de los puntos de control del aeropuerto mencionados anteriormente.

El Comité concluye que el podría considerarse que las medidas elegidas han cumplido el principio de necesidad si el responsable del tratamiento puede demostrar que no existen soluciones alternativas menos intrusivas que podrían lograr el mismo objetivo con la misma eficacia. Además, el carácter intrusivo del tratamiento puede contrarrestarse con la participación activa de los pasajeros, ya que su plantilla biométrica se almacena en manos de la propia persona, por ejemplo, en su dispositivo individual, bajo su control exclusivo, y sus datos se eliminan poco después de que se complete el cotejo. Sobre esta base, el Comité concluye que el tratamiento previsto en el primer supuesto **podría considerarse en principio compatible con los artículos 5, apartado 1, letra f), y 25 y 32 del RGPD**, siempre que se apliquen las garantías adecuadas.

El Comité ha identificado salvaguardas que, como mínimo, deberían aplicarse para lograr una solución similar a la del primer escenario.

El **segundo escenario** implica el almacenamiento centralizado, dentro del aeropuerto, de una plantilla biométrica de forma encriptada con una clave/secreto únicamente en poder del pasajero. Esto permite la

autenticación de los pasajeros (comparación 1:1) a medida que pasan por los puntos de control del aeropuerto mencionados anteriormente. La inscripción es válida durante un período determinado, que, por ejemplo, puede ser de hasta un año desde que se tomó el último vuelo hasta la fecha de vencimiento del pasaporte.

El Comité concluye que podría considerarse que el tratamiento ha cumplido el principio de necesidad si el responsable del tratamiento puede demostrar que no existen soluciones alternativas menos intrusivas que podrían lograr el mismo objetivo con la misma eficacia. Además, la intrusión del tratamiento puede ser contrarrestada por la participación activa del pasajero, ya que tiene bajo su control exclusivo la clave/secreto de sus datos biométricos cifrados. Suponiendo que el responsable del tratamiento aplique las salvaguardas adecuadas, los riesgos para la seguridad derivados del uso de una base de datos centralizada en este escenario podrían mitigarse y el impacto negativo en los derechos y libertades fundamentales de los interesados podría considerarse proporcional al beneficio previsto. En cuanto al principio de limitación del almacenamiento, no se ha facilitado a el Comité información que justifique el largo período de almacenamiento. Con el fin de lograr la compatibilidad con el artículo 5, apartado 1, letra e) del RGPD en este escenario, los responsables del tratamiento deben poder justificar por qué el período de conservación previsto es necesario para tal fin en casos específicos. El Comité recomienda que los responsables prevean el período de almacenamiento más corto posible, al tiempo que ofrecen a los pasajeros la opción de establecer su período de almacenamiento preferido. Sobre esta base, el Comité concluye que el tratamiento previsto en el escenario 2 podría considerarse en principio compatible con los artículos 5, apartado 1, letras e), y f), 25 y 32 del RGPD, siempre que se apliquen las garantías adecuadas.

El Comité ha identificado salvaguardas que, como mínimo, deberían implementarse para una solución similar a la del segundo escenario.

El **tercer escenario** implica el almacenamiento centralizado de una plantilla biométrica encriptada dentro del aeropuerto bajo el control del operador aeroportuario. Esto permite la identificación de los pasajeros (comparación 1:N) a medida que avanzan a través de los puntos de control del aeropuerto mencionados anteriormente. El período de almacenamiento en este escenario suele ser de 48 horas y los datos se eliminan una vez que el avión ha despegado.

Dado que el almacenamiento de los datos de identidad y biométricos se realiza en una base de datos centralizada, si la confidencialidad de la base de datos se ve comprometida, puede implicar el acceso a todo el conjunto de datos y podría permitir la identificación no autorizada o ilícita de los pasajeros en otros escenarios. La arquitectura de almacenamiento centralizado bajo el control del operador aeroportuario también hace que el pasajero pierda en mayor medida el control de sus datos. El Comité considera que se puede lograr un resultado similar a la racionalización del flujo de pasajeros en los aeropuertos de una manera menos intrusiva y que el impacto negativo en los derechos y libertades fundamentales de los interesados que se derivaría de una brecha de datos en una base de datos centralizada de datos biométricos parece superar el beneficio previsto del tratamiento. Por lo tanto, el tratamiento no puede cumplir con los principios de necesidad y proporcionalidad. Sobre esta base, el Comité concluye que el tratamiento previsto en el tercer supuesto no puede ser compatible con el artículo 25 del RGPD. Además, no cumpliría con los artículos 5, apartado 1, letra f), y 32 del RGPD si un responsable del tratamiento se limitara a las medidas descritas en este escenario.

El **cuarto escenario** implica el almacenamiento centralizado de una plantilla biométrica inscrita de forma cifrada en la nube bajo el control de la compañía aérea o su proveedor de servicios en la nube. Esto permite la identificación de los pasajeros (comparación 1:N) a medida que avanzan a través de los puntos de control

del aeropuerto mencionados anteriormente. El período de almacenamiento en este escenario puede ser potencialmente durante el tiempo que el cliente tenga una cuenta con la compañía aérea.

Dado que el almacenamiento de los datos de identificación y biométricos se realiza en una base de datos central en la nube, varias entidades podrían tener acceso a dichos datos, incluidos posiblemente proveedores no pertenecientes al EEE. Los datos del pasajero se descifran cuando están en uso y las claves están bajo el control de la compañía aérea o sus encargados, lo que podría aumentar la superficie de exposición de seguridad. Esta arquitectura centralizada de almacenamiento también hace que el pasajero pierda el control de sus datos en mayor medida. Los datos también podrían almacenarse durante un período de tiempo significativo, lo que expone a los datos a mayores riesgos a producirse una brecha de seguridad y parece ir más allá de lo estrictamente necesario y proporcionado para los fines del tratamiento, a menos que se tomen medidas adicionales para mitigar los riesgos para las personas.

El Comité considera que se puede lograr un resultado similar a la racionalización del flujo de pasajeros en los aeropuertos de una manera menos intrusiva y que el impacto negativo en los derechos y libertades fundamentales de los interesados que podría derivarse de una brecha de datos en una base de datos centralizada de datos biométricos parece superar el beneficio previsto del tratamiento. Por lo tanto, el tratamiento no puede cumplir con los principios de necesidad y proporcionalidad. Sobre esta base, el Comité concluye que el tratamiento previsto en el cuarto supuesto **no puede ser compatible con el artículo 25 del RGPD**. Además, **no cumpliría con el artículo 5, apartado 1, letra e) del RGPD** sobre la base de la información de que dispone el Comité y **no cumpliría con los artículos 5, apartado 1, letra f), y 32 del RGPD** si un responsable del tratamiento se limitara a las medidas descritas en este escenario.

Índice

1	INTRODUCCIÓN	6
1.1	Resumen de los hechos.....	6
1.2	Admisibilidad de la solicitud de dictamen con arreglo al artículo 64, apartado 2, del RGPD	8
2	ÁMBITO DE APLICACIÓN Y CONTEXTO DEL DICTAMEN	9
2.1	Alcance del dictamen	9
2.2	Nociones clave.....	12
3	SOBRE EL FONDO DE LA SOLICITUD	14
3.1	Observaciones generales	14
3.2	Compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD	16
3.2.1	Escenario 1: almacenamiento de la plantilla biométrica solo en manos del pasajero, para autenticación.....	16
3.2.2	Escenario 2: almacenamiento centralizado de la plantilla biométrica cifrada dentro del aeropuerto y con una llave/secreto únicamente en manos del pasajero para su autenticación	24
3.2.3	Almacenamiento centralizado de las plantillas biométricas para su identificación.....	28
3.2.3.1	<i>Escenario 3.1: almacenamiento centralizado en una base de datos dentro del aeropuerto, bajo el control del operador aeroportuario</i>	<i>29</i>
3.2.3.2	<i>Escenario 3.2: almacenamiento centralizado en una nube, bajo el control de la compañía aérea</i>	<i>32</i>
4	CONCLUSIONES	34

El Comité Europeo de Protección de Datos

Vistos el artículo 63 y el artículo 64, apartado 2, del Reglamento (UE) 2016/679/UE del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, «**RGPD**»),

Visto el Acuerdo EEE y, en particular, su anexo XI y su Protocolo 37, modificados por la Decisión del Comité Mixto del EEE nº 154/2018, de 6 de julio de 2018¹,

Vistos los artículos 10 y 22 del Reglamento interno del Comité Europeo de Protección de Datos (en lo sucesivo, el «**Comité**» o el «**CEPD**»),

Considerando que:

(1) La función principal del Comité es garantizar la aplicación coherente del RGPD en todo el Espacio Económico Europeo (en adelante, "**EEE**"). El artículo 64, apartado 2, del RGPD establece que cualquier autoridad de control (en lo sucesivo, «**AC**»), el presidente del Comité o la Comisión Europea podrán solicitar que cualquier asunto de aplicación general o que produzca efectos en más de un Estado miembro del EEE sea examinado por el Comité con el fin de obtener un dictamen.

(2) El Dictamen del Comité se adoptará de conformidad con el artículo 64, apartado 3, del RGPD, en relación con el artículo 10, apartado 2 del Reglamento interno del CEPD en un plazo de ocho semanas a partir de la fecha en que el presidente y la autoridad competente hayan decidido que el expediente está completo. Por decisión del presidente, este plazo podrá prorrogarse por otras seis semanas teniendo en cuenta la complejidad del asunto.

ha aprobado el presente dictamen:

1 INTRODUCCIÓN

1.1 Resumen de los hechos

1. El 16 de febrero de 2024, la Autoridad de Control francesa (en lo sucesivo, « **AC FR** ») solicitó a el Comité que emitiera un dictamen sobre la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD sobre el uso de la tecnología de reconocimiento facial por parte de los operadores aeroportuarios y las compañías aéreas para la autenticación o identificación biométrica de los pasajeros², con el fin de agilizar el flujo de pasajeros, en los puntos de control de seguridad del aeropuerto³, entrega de equipaje, embarque y acceso a la sala de pasajeros (excluidos los controles fronterizos y los controles realizados por las tiendas libres

¹ Las referencias a los "**Estados miembros**" que se hacen a lo largo del presente dictamen deben entenderse como referencias a los "Estados miembros del EEE". Las referencias a la "Unión" o a la "UE" que se hacen a lo largo del presente dictamen deben entenderse hechas al "EEE".

² En el contexto de las presentes conclusiones, se entenderá por "**pasajero**" un interesado cuyos datos personales se traten para la finalidad específica descrita en el presente dictamen. En lo sucesivo, en el presente dictamen, los términos "pasajero" e "individuo" son utilizados indistintamente.

³ A efectos del presente dictamen, se entenderá por "**controles de seguridad aeroportuarios**" los controles de seguridad efectuados bajo la responsabilidad del gestor aeroportuario a los que deben someterse los pasajeros para acceder desde la zona de salidas a la zona de embarque o a la puerta de embarque.

de impuestos) (en adelante, la "**Solicitud**"). FR AC adjuntó a su solicitud una descripción de los casos de uso típicos (anexo I).

2. En su solicitud, la AC FR señala que los modelos que se están probando actualmente en varios aeropuertos de la Unión varían de un Estado miembro a otro, lo que puede crear un riesgo de divergencia entre las interpretaciones entre las AC y un riesgo de que se produzcan efectos diferentes para los derechos y libertades fundamentales de los interesados en la Unión⁴.

3. El Comité considera que, para dar respuesta a la solicitud, es necesario responder a las siguientes preguntas:

4. **Pregunta 1:**

1.1. El uso de tecnología de reconocimiento facial biométrico para autenticación con el **fin específico de racionalizar el flujo de pasajeros en los aeropuertos** (controles de seguridad, entrega de equipaje, embarque y acceso a la sala de pasajeros) ¿Puede ser compatible con el **artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD**, en el caso de una arquitectura de almacenamiento, en la que la plantilla biométrica de cada pasajero se almacena **únicamente en manos de la persona?**, por ejemplo, localmente en su dispositivo individual, ¿bajo su control exclusivo?

1.2. En caso de que dicho tratamiento se considerara compatible con las disposiciones antes mencionadas, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

Pregunta 2:

2.1. El uso de tecnología de reconocimiento facial biométrico para autenticación o identificación con el **fin específico de racionalizar el flujo de pasajeros en los aeropuertos** (controles de seguridad, entrega de equipaje, embarque y acceso a la sala de pasajeros) ¿Puede ser compatible con el **artículo 5, apartado 1, letras e) y f), y con los artículos 25 y 32 del RGPD** en el caso de una arquitectura centralizada de almacenamiento, donde la plantilla biométrica de cada pasajero se almacena en una base de datos central:

2.1.1. ¿En una base de datos centralizada dentro del aeropuerto, bajo el control del operador aeroportuario, de forma encriptada, con una clave/secreto en poder exclusivo de la persona (por ejemplo, en el teléfono móvil de la persona), para su autenticación?

2.1.2. En caso de que dicho tratamiento se considere compatible, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

2.2.1. ¿En una base de datos centralizada dentro del aeropuerto, bajo el control del operador aeroportuario, de forma cifrada, con claves en poder del gestor aeroportuario, para su identificación?

2.2.2. En caso de que dicho tratamiento se considere compatible, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

2.3.1 ¿En la nube, bajo el control de la compañía aérea o de su proveedor de servicios (encargado del tratamiento), de forma encriptada, con claves en poder de la compañía aérea o su proveedor de servicios, para su identificación?

⁴ Solicitud, p. 1.

2.3.2. En caso de que dicho tratamiento se considerara compatible, ¿qué garantías mínimas adecuadas serían necesarias, a la luz de los artículos 25 y 32 del RGPD?

5. Después de que la AC FR considerara que el expediente estaba completo el 16 de febrero de 2024 y la presidenta del Comité considerara que el expediente estaba completo el 23 de febrero de 2024, la Secretaría distribuyó el expediente. La presidenta del Comité decidió, de conformidad con el artículo 64, apartado 3, del RGPD en relación con el artículo 10, apartado 2 del Reglamento interno del CEPD, prorrogar el plazo por defecto de ocho semanas por otras seis semanas debido a la complejidad de la materia.

1.2 Sobre la admisibilidad de la solicitud de dictamen con arreglo al artículo 64, apartado 2, del RGPD

6. El artículo 64, apartado 2 del RGPD establece, en particular, que cualquier AC podrá solicitar que el Comité examine cualquier asunto de alcance general o que produzca efectos en más de un Estado miembro con el fin de obtener un dictamen.
7. El Comité considera que la solicitud planteada por la AC FR sobre la compatibilidad del uso de la tecnología de reconocimiento facial para la autenticación o identificación biométrica con el fin específico de racionalizar el flujo de pasajeros en los aeropuertos se refiere a cuestiones que "producen efectos en más de un Estado miembro", porque, como se explica en la solicitud⁵, actualmente hay varios proyectos en desarrollo en los aeropuertos de los Estados miembros, y se estima que dicho uso aumentará en los próximos años. Los modelos que actualmente están siendo probados por diferentes aeropuertos y compañías aéreas varían significativamente de un Estado miembro a otro, lo que puede crear el riesgo de que, desde el punto de vista de la protección de datos, se produzcan efectos divergentes en más de un Estado miembro.
8. Asimismo, el Comité considera que la solicitud remitida por la AC FR tiene consecuencias importantes para la aplicación de los principios establecidos en el artículo 5, apartado 1, letras e) y f) del RGPD, y los requisitos aplicables a los responsables del tratamiento en virtud del artículo 25 del RGPD, así como los requisitos aplicables a los responsables y encargados del tratamiento en virtud del artículo 32 del RGPD. Por lo tanto, la presente solicitud se refiere a una «cuestión de aplicación general» en el sentido del artículo 64, apartado 2, del RGPD, en la medida en que se refiere a la interpretación coherente de los principios de limitación del almacenamiento (artículo 5, apartado 1, letra e) del RGPD) y de integridad y confidencialidad (artículo 5, apartado 1, letra f) del RGPD), así como de los conceptos de protección de datos desde el diseño y por defecto (artículo 25 del RGPD) y de seguridad de los datos (artículo 32 del RGPD) para garantizar, entre otros, la aplicación coherente de dichas disposiciones en el EEE.
9. Cualquier posible divergencia de posiciones entre los Estados miembros sobre la interpretación del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD amplificaría el riesgo de que los operadores aeroportuarios y las compañías aéreas desarrollen proyectos de reconocimiento facial de manera no coherente. Dado que la AC FR ha demostrado la clara necesidad de una interpretación coherente de estas disposiciones en relación con la tecnología de reconocimiento facial para la autenticación o identificación biométrica de los pasajeros, con el fin de racionalizar el flujo de pasajeros en los aeropuertos⁶, el Comité considera que la solicitud está motivada, en consonancia con el artículo 10, apartado 3 del Reglamento interno del CEPD.

⁵ Solicitud, p. 3.

⁶ Solicitud, p. 1-3.

10. De conformidad con el artículo 64, apartado 3 del RGPD, el CEPD no emitirá dictamen si ya lo ha hecho⁷. El CEPD aún no ha respondido a las preguntas planteadas a raíz de la solicitud.

Aunque las Directrices 3/2019 del CEPD sobre dispositivos de vídeo⁸ ya proporcionan algunos elementos útiles sobre las medidas de seguridad que deben aplicarse al tratamiento de datos biométricos, no abordan todos los aspectos relativos a las cuestiones planteadas en la Solicitud. Además, las orientaciones disponibles del CEPD, incluidas las Directrices 3/2019 del CEPD sobre dispositivos de vídeo, no proporcionan orientaciones específicas sobre los posibles elementos que deben verificarse en relación con el almacenamiento centralizado o descentralizado de datos biométricos para identificar o autenticar a los pasajeros con el fin de agilizar el flujo de pasajeros en los aeropuertos, ni sobre la compatibilidad de dicho tratamiento con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD.

11. Por estas razones, el Comité considera que la solicitud es admisible y que las cuestiones planteadas deben analizarse en un dictamen adoptado de conformidad con el artículo 64, apartado 2 del RGPD.

2 ÁMBITO DE APLICACIÓN Y CONTEXTO DEL DICTAMEN

2.1 Alcance del dictamen

12. El presente dictamen se refiere únicamente a la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD del uso de la tecnología de reconocimiento facial para la autenticación o identificación de pasajeros mediante la biometría por parte de los operadores aeroportuarios y las compañías aéreas, **con el fin específico de racionalizar el flujo de pasajeros en los aeropuertos**, a saber, en los controles de seguridad, la entrega de equipajes, embarque y acceso a la sala de pasajeros, según la Solicitud.

13. Con respecto al **alcance de esta Opinión**, el Comité aclara lo siguiente:

- 1) El tratamiento de datos personales en el marco de los controles fronterizos y los controles efectuados por las tiendas libres de impuestos no entra en el ámbito de aplicación del presente dictamen, ya que son llevados a cabo por responsables del tratamiento distintos de los operadores aeroportuarios y las compañías aéreas.
- 2) El uso de la tecnología de reconocimiento facial, incluso si se basa en los escenarios descritos a continuación en la sección 3.2, para cualquier otro fin (como la aplicación de la ley) o por cualquier otra parte, aunque sea con fines similares, queda fuera del ámbito de aplicación del presente dictamen.
- 3) El presente dictamen solo examina el tratamiento de los datos personales de los pasajeros y no abarca otros tipos de interesados, como el personal de los operadores aeroportuarios o de las compañías aéreas.
- 4) Las presentes conclusiones examinan la solicitud presentada por FR SA en relación con la compatibilidad de las arquitecturas de almacenamiento de las plantillas biométricas de los pasajeros con el artículo 5, apartado 1, letras e) y f), y con los artículos 25 y 32 del RGPD. En este sentido, el presente Dictamen no incluye un análisis exhaustivo y completo sobre el cumplimiento del RGPD, por parte del responsable o responsables pertinentes en cada caso, así como de su(s) encargado(s), en su caso. Esto es especialmente importante si se tiene en cuenta que estas tecnologías conllevan un muy alto riesgo asociados al

⁷ Artículo 64, apartado 3, del RGPD y artículo 10, apartado 4, del Reglamento interno del CEPD.

⁸ Directrices 3/2019 del CEPD sobre el tratamiento de datos personales a través de dispositivos de vídeo, versión 2.0, adoptadas el 29 de enero de 2020 (en adelante, «**Directrices del CEPD 3/2019 sobre dispositivos de vídeo**»).

tratamiento de las categorías especiales de datos de conformidad con el artículo 9 del RGPD. Por lo tanto, el presente dictamen se entiende sin perjuicio de una evaluación relativa a otras disposiciones del RGPD en lo que respecta al uso de tecnologías de reconocimiento facial, incluso en el sector específico al que se refiere la presente solicitud, el análisis jurídico y técnico correspondiente a un determinado tratamiento contemplará las circunstancias específicas previstas por el responsable del tratamiento en cada caso concreto.

- 5) El presente dictamen no examina el tratamiento de los datos personales de los menores y se entiende sin perjuicio de los requisitos específicos aplicables a este respecto.
 - 6) El presente dictamen se entiende sin perjuicio de los requisitos legales y de otras restricciones al uso de datos biométricos derivados de las legislaciones nacionales de los Estados miembros⁹.
 - 7) Las conclusiones que se expongan en el presente dictamen se entenderán sin perjuicio de la evolución tecnológica que se produzca al respecto.
 - 8) En el presente Dictamen se examinan cuatro supuestos, cuyas características específicas se describen más adelante en la sección 3.2. No aborda otros escenarios, incluso si el tratamiento se realiza con los mismos fines.
14. En su solicitud, la AC FR indicó que el tratamiento de los datos biométricos de los pasajeros con el fin de racionalizar el flujo de pasajeros en los aeropuertos se basaría en la presunción de que las personas dan su consentimiento a dicho tratamiento, lo que posiblemente constituiría la base jurídica en virtud del RGPD¹⁰. **Sin embargo, el análisis de la base jurídica aplicable no entra en el ámbito de las cuestiones planteadas al CEPD en la solicitud y, por lo tanto, la validez del consentimiento para dicho tratamiento de conformidad con los artículos 6, 7 y 9 del RGPD no se examina en el presente dictamen.**
15. No obstante, el CEPD señala, en términos generales, que, si los responsables del tratamiento pertinentes se basaran en esta base jurídica, tendrían que obtener un consentimiento explícito válido¹¹ de las personas que deseen utilizar dichos servicios. Ese consentimiento explícito tendría que ser libre, específico e informado,¹² y la cuestión de si se cumplen esas condiciones se analizaría caso por caso. Esto significa, *inter alia*, que:
- 1) Las personas tendrían que poder retirar fácilmente dicho consentimiento en cualquier momento y sin perjuicio alguno¹³.
 - 2) Para que el consentimiento pueda darse libremente, dicho uso de tecnologías biométricas solo puede tener lugar de forma voluntaria, ya que las personas deben poder elegir libremente si desean o no utilizar

⁹ Por ejemplo, el artículo 9, apartado 4, del RGPD establece que los Estados miembros pueden mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos biométricos.

¹⁰ Solicitud, Anexo I.

¹¹ De conformidad con los artículos 4, apartado 14, y 9, apartado 1, del RGPD, así como con el artículo 9, apartado 2, letra a) del RGPD, queda prohibido el tratamiento de datos biométricos con el fin de identificar de forma unívoca a una persona física, a menos que el interesado haya dado su consentimiento explícito para el tratamiento de dichos datos personales para uno o varios fines específicos, salvo cuando el Derecho de la Unión o de los Estados miembros disponga que la prohibición a que se refiere el artículo 9, apartado 1, del RGPD no podrá ser levantado por el interesado. Véanse también los considerandos 51, 52 y 53 del RGPD.

¹² Artículos 4, apartado 11, y 7 del RGPD.

¹³ Artículo 7, apartado 4, del RGPD, así como considerando 50 del RGPD.

estos servicios y sin ningún detrimento (como retrasos significativamente más largos para los pasajeros que no dan su consentimiento¹⁴), incentivos, costes o ventajas adicionales a cambio¹⁵.

- 3) También sería necesario solicitar el consentimiento explícito de las personas cuyos datos biométricos se procesan, incluso si no se han inscrito para ser identificadas o autenticadas por dichos medios. En otras palabras, es esencial que las personas que no dieron su consentimiento explícito para el reconocimiento facial para el propósito previsto no tengan sus rostros escaneados por las cámaras. Esto puede lograrse, por ejemplo, dedicando carriles específicos al reconocimiento facial y proporcionando una señalización adecuada y una separación física con los flujos de control no biométricos para permitir una identificación clara de dichos carriles.
 - 4) Sin perjuicio de si el consentimiento fuera la base jurídica aplicable para dicho tratamiento, los principios de tratamiento consagrados en el artículo 5 del RGPD con respecto a la necesidad y la proporcionalidad, siguen aplicándose incluso cuando las personas hayan dado su consentimiento explícito para el uso de sus datos biométricos¹⁶.
16. En la solicitud se especifica¹⁷ que los operadores aeroportuarios actuarían como responsables en lo que respecta al tratamiento en los puntos de control de seguridad de los aeropuertos, mientras que las compañías aéreas actuarían como responsables en lo que respecta al tratamiento en la entrega de equipaje, el embarque y el acceso a la sala de pasajeros. Por lo tanto, el Comité observa que diferentes actores podrían estar involucrados en el tratamiento descrito en la solicitud y no ha evaluado la aplicación de los roles conjuntos de responsable y/o encargado en los escenarios que se describen a continuación en la sección 3.2 de esta opinión. En cada caso, es necesario identificar a los actores implicados y asignar claramente sus responsabilidades, para que se cumplan los requisitos del RGPD¹⁸.
17. Además, el Comité observa que actualmente no existe un requisito legal uniforme en la UE para que los operadores aeroportuarios y las compañías aéreas identifiquen a los pasajeros y verifiquen que el nombre que figura en la tarjeta de embarque del pasajero coincide con el nombre que figura en su documento de identidad en todos los puntos de control mencionados¹⁹. Por lo tanto, tales requisitos están sujetos a legislaciones nacionales que pueden variar de un Estado miembro a otro. En algunos Estados miembros, dicha verificación puede ser necesaria para algunos puntos de control (p. ej. entrega de equipaje o embarque), mientras que en

¹⁴ Por ejemplo, esto podría incluir consideraciones como el diseño de un sistema para evitar crear presión social sobre los pasajeros que no quieren dar su consentimiento, evitando que su elección tenga un impacto negativo en otros pasajeros.

¹⁵ Directrices 05/2020 del CEPD sobre la autorización con arreglo al Reglamento (UE) 2016/679, versión 1.1, adoptadas el 4 de mayo de 2020 (en lo sucesivo, «**Directrices 5/2020 del CEPD sobre el consentimiento**»), párrafos 46 y 48.

¹⁶ Ídem, párrafo 5.

¹⁷ Solicitud, Anexo I.

¹⁸ De conformidad con los artículos 4, apartados 7 y 8, 5, apartado 2, y los artículos 24, 26, 28 y 29 del RGPD. Véanse también las Directrices 07/2020 del CEPD sobre los conceptos de responsable y encargado del tratamiento en el RGPD, versión 2.1, adoptadas el 7 de julio de 2021.

¹⁹ El Reglamento pertinente a nivel de la UE es el Reglamento de Ejecución (UE) 2015/1998 de la Comisión, de 5 de noviembre de 2015, por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea. Sin embargo, este Reglamento no aborda los controles de los documentos de identidad oficiales en los puestos de control de los aeropuertos, y los Estados miembros tienen la facultad discrecional de regularlo a nivel nacional.

otros no se requieren tales controles en la actualidad²⁰. La existencia de obligaciones legales para verificar la identidad de los pasajeros tiene un impacto directo en las prácticas de los diferentes aeropuertos.

18. Por consiguiente, en estas situaciones, en **las que no se requiere la verificación de la identidad de los pasajeros con un documento oficial de identidad, no debe realizarse ninguna verificación con el uso de datos biométricos, ya que esto daría lugar a un tratamiento excesivo de los datos, implicando así un tratamiento de datos adicionales en comparación con la situación actual e iría más allá de lo necesario para la finalidad pertinente comparado con la situación actual, infringiendo el principio de minimización de datos establecido en el artículo 5, apartado 1, letra c) del RGPD**. Esta consideración debe tenerse en cuenta en relación con el examen de todos los supuestos que se describen a continuación en la sección 3.2 del presente dictamen.

2.2 Nociones clave

19. Para que se consideren datos biométricos con arreglo al artículo 4, punto 14 del RGPD²¹, el tratamiento de datos relativos a las características físicas, fisiológicas o de comportamiento de una persona física, debe implicar una medición de estas características, ya que los datos biométricos son el resultado de dichas mediciones²².
20. Mediante el uso de la imagen de la cara de un individuo (una fotografía o un vídeo) llamada "**muestra**" biométrica, es posible extraer una representación digital de las distintas características de dicha cara (esto se denomina "**plantilla**").²³ Además, el Comité recuerda que "una plantilla biométrica es una representación digital de las características únicas que se han extraído de una muestra biométrica y que pueden almacenarse en una base de datos biométrica"²⁴ que permiten o confirman la identificación única de una persona física. Además, "se supone que esta plantilla biométrica es única y específica para cada individuo y es, en principio, permanente en el tiempo".²⁵ Normalmente, en un proceso de comparación destinado a identificar o autenticar a una persona mediante el reconocimiento facial, una plantilla biométrica entrante se compara con los objetos almacenados para verificar una coincidencia o encontrar una en una base de datos²⁶.

²⁰ Lo que significa que actualmente no se realiza ninguna verificación o solo se verifica la existencia de la tarjeta de embarque. Por ejemplo, sobre la base del Protocolo relativo a la exención de los nacionales de Dinamarca, Finlandia, Noruega y Suecia de la obligación de tener un pasaporte o un permiso de residencia mientras residan en un país escandinavo distinto del suyo, de 22 de mayo de 1954, a partir del 1º de julio de 1954, los ciudadanos de Noruega, Dinamarca, Finlandia y Suecia están exentos de la obligación de poseer un pasaporte u otro documento de identidad de viaje cuando viajen entre esos países.

²¹ Véanse también los considerandos 51, 52 y 53 del RGPD.

²² Directrices del CEPD n.º 3/2019 sobre dispositivos de vídeo, párrafo 74.

²³ Directrices 05/2022 del CEPD sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley, versión 2.0, adoptadas el 26 de abril de 2023 (en lo sucesivo, «**Directrices 5/2022 del CEPD sobre el reconocimiento facial en las fuerzas y cuerpos de seguridad**»), párrafos 7 y 8.

²⁴ Ídem, párrafo 9.

²⁵ Ídem.

²⁶ Directrices 5/2022 del CEPD sobre el reconocimiento facial en la aplicación de la ley, apartados 10 y 11; véase también la norma internacional ISO/IEC 2382-37, 2022-03, disponible en:

[https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%20238237_2022\(E\).zip](https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%20238237_2022(E).zip) [consultado por última vez el 23 de mayo de 2024] (en adelante, "**ISO/IEC 2382-37**")

21. La tecnología de reconocimiento facial puede cumplir dos funciones distintas: autenticación²⁷ e identificación²⁸. Si bien ambas funciones son distintas, ambas se basan en el tratamiento de datos biométricos relativos a una persona física identificada o identificable²⁹ y, por tanto, constituyen un tratamiento de categorías especiales de datos personales en virtud del artículo 9 del RGPD³⁰.
22. En particular:
- La autenticación** tiene como objetivo confirmar una declaración biométrica a través de la comparación. Esto también se denomina verificación 1 a 1.
- La identificación** tiene como objetivo buscar en una base de datos de registros biométricos para devolver identificadores atribuibles a un solo individuo. Esto también se denomina identificación de 1 a muchos.
23. En ambos casos (es decir, identificación y autenticación), las técnicas de reconocimiento facial se basan en una coincidencia estimada entre las plantillas, es decir, la que se compara y la(s) registrada(s). Desde este punto de vista, son probabilísticos: la comparación deduce una mayor o menor probabilidad de que la persona sea efectivamente la persona que se pretende autenticar o identificar; si esta probabilidad supera un determinado umbral en el sistema, definido por el usuario o el desarrollador del sistema, el sistema asumirá que hay una coincidencia que debe identificarse o autenticarse³¹.

²⁷ El Comité observa que el próximo Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) (aún no publicado en el Diario Oficial) también define en su artículo 3, apartado 36, la «verificación biométrica» como «la verificación automatizada e individualizada, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados anteriormente» (véase la legislación del Parlamento Europeo Resolución, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C90146/2021 – 2021/0106(COD)]).

²⁸ Ídem, el artículo 3, apartado 35, de la Ley de Inteligencia Artificial define la «identificación biométrica» como «el reconocimiento automatizado de características humanas físicas, fisiológicas, conductuales o psicológicas con el fin de establecer la identidad de una persona física comparando los datos biométricos de esa persona con los datos biométricos de las personas almacenados en una base de datos».

²⁹ ISO/IEC 2382-37.

³⁰ Artículo 4, apartado 14, del RGPD y Directrices 5/2022 del CEPD sobre el reconocimiento facial en la aplicación de la ley, párrafo 12.

³¹ Directrices 5/2022 del CEPD sobre el reconocimiento facial en las fuerzas y cuerpos de seguridad, párrafo 11. Véase también ISO/IEC 2382-37.

3 SOBRE EL FONDO DE LA SOLICITUD

3.1 Observaciones generales

24. En esta sección se analizan las cuestiones planteadas en el párrafo 4 *supra*. En este contexto, el Comité analizará, para la pregunta 1, la compatibilidad con el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD, y con la pregunta 2, la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD.
25. Para ello, el Comité analizará cuatro escenarios diferentes³², cuyas características específicas se describen a continuación en el apartado 3.2.
26. Como observación preliminar, el Comité recuerda que el uso de datos biométricos y, en particular, de la tecnología de reconocimiento facial entraña un muy alto riesgo para los derechos y libertades de los interesados. En primer lugar, el tratamiento de que se trata se refiere a los datos biométricos a los que se concede una protección especial en virtud del artículo 9 del RGPD. En particular, los datos biométricos cambian irreversiblemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean "legibles por máquina" y estén sujetas a un uso posterior³³. Además, el uso de la tecnología de reconocimiento facial puede dar lugar a riesgos asociados con falsos negativos, sesgos y discriminación,³⁴ y el potencial de uso indebido de datos biométricos podría tener graves consecuencias para las personas, como el fraude de identidad o la suplantación de identidad³⁵. También hay que tener en cuenta que, cuando el reconocimiento facial se realiza a distancia y sin la participación activa del interesado, las personas pueden ser aún menos conscientes de dicho tratamiento y de los riesgos asociados. Por último, es importante destacar que las características en las que se basan los datos biométricos pueden considerarse generalmente como permanentes y deben tratarse como no revocables, especialmente en el contexto del reconocimiento facial³⁶.
27. Por lo tanto, teniendo en cuenta lo anterior, antes de utilizar dichas tecnologías, incluso si se consideraran especialmente eficaces, los responsables del tratamiento deben evaluar el impacto en los derechos y libertades fundamentales de los interesados y considerar si medios menos intrusivos pueden lograr su propósito legítimo del tratamiento³⁷.

³² Los cuatro escenarios analizados por el Comité se basan en los casos de uso presentados en el anexo I de la solicitud. La AC FR ha aclarado que los casos de uso presentados en el Anexo I de la Solicitud son ejemplos de implementación, pertenecientes a un escenario, utilizados con fines ilustrativos.

³³ Artículo 29 Dictamen 3/2012 del Grupo de Trabajo sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012, WP193 (en lo sucesivo, «**Dictamen 3/2012 del Grupo de Trabajo del artículo 29 sobre tecnologías biométricas**»), p. 4. Cabe señalar que el presente dictamen se refiere a la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos («Directiva sobre protección de datos»). El RGPD ha ampliado el alcance de las categorías especiales de datos y, a diferencia de la Directiva de Protección de Datos, el RGPD establece que los datos biométricos son categorías especiales de datos (artículo 9 del RGPD).

³⁴ Directrices sobre reconocimiento facial, Comité Consultivo del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos personales, junio de 2021, p. 15; también las Directrices 5/2022 del CEPD sobre el reconocimiento facial en la aplicación de la ley, apartado 27.

³⁵ Artículo 29 Dictamen 3/2012 del WP sobre tecnologías biométricas, p. 29.

³⁶ Directrices 5/2022 del CEPD sobre el reconocimiento facial en las fuerzas y cuerpos de seguridad, párrafo 104.

³⁷ Considerando 39 del RGPD. Véanse también las Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 73.

28. El Comité también recuerda que el derecho a la protección de los datos personales no es un derecho absoluto y debe equilibrarse con otros derechos fundamentales protegidos por la Carta, de conformidad con el principio de proporcionalidad³⁸.
29. El artículo 25, apartado 1 del RGPD se refiere a «los principios de protección de datos» que se enumeran en el artículo 5 del RGPD³⁹ y exige aplicarlos desde el diseño «de manera efectiva»⁴⁰. Esto incluye expresamente el principio de minimización de datos previsto en el artículo 5, apartado 1, letra c) del RGPD,⁴¹ que exige que los datos personales sean “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan, dando expresión al principio de proporcionalidad”⁴². Además, el artículo 25, apartado 2, del RGPD especifica la obligación de “minimización de datos por defecto”, al precisar que se aplica a la cantidad de datos personales recogidos, el alcance de su tratamiento, el período de conservación y su accesibilidad⁴³.
30. Sin embargo, el artículo 25 del RGPD no exige a los responsables del tratamiento que apliquen ninguna medida técnica y organizativa específica, sino que las medidas y garantías elegidas sean específicas para el contexto y los riesgos para los derechos y libertades del interesado que plantea el tratamiento⁴⁴. Del mismo modo, el artículo 32 del RGPD sobre la seguridad del tratamiento exige a los responsables y encargados del tratamiento que apliquen las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas.
31. Es importante destacar que, incluso si los pasajeros dieran su consentimiento explícito para el uso de sus datos biométricos con el fin de racionalizar el flujo de pasajeros en los aeropuertos, los principios de tratamiento consagrados en el RGPD relativos a la necesidad y la proporcionalidad siguen aplicándose y deben cumplirse⁴⁵.

³⁸ Considerando 4 del RGPD. Véase también, a este respecto, la sentencia del Tribunal de Justicia de 22 de junio de 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504 (en lo sucesivo, «*Latvijas Republikas Saeima*, C-439/19»), apartados 98, 110 y 113. Además, el principio de proporcionalidad, como principio general del Derecho de la Unión, exige que las medidas ejecutadas mediante actos de la Unión sean adecuadas para alcanzar el objetivo perseguido y no vayan más allá de lo necesario para alcanzarlo (véanse las sentencias del Tribunal de Justicia de 9 de noviembre de 2010, *Volker und Markus Schecke y Eifert*, C-92/09 y C-93/09, ECLI:EU:C:2010:662 (en lo sucesivo, “C-92/09 y C-93/09, *Volker und Schecke*”), apartado 74 y jurisprudencia citada.

³⁹ Directrices 4/2019 del CEPD sobre el artículo 25 de la protección de datos desde el diseño y por defecto, versión 2.0, adoptadas el 20 de octubre de 2020 (en adelante, «Directrices del CEPD 4/2019 sobre la protección de datos desde el diseño y por defecto»), párrafo 11.

⁴⁰ El artículo 25, apartado 1, del RGPD establece que: «Teniendo en cuenta el estado de la técnica, el coste de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas que plantea el tratamiento, el responsable del tratamiento, tanto en el momento de la determinación de los medios de tratamiento como en el momento del propio tratamiento deberá aplicar las medidas técnicas y organizativas adecuadas, como la seudonimización, que tengan por objeto aplicar los principios de protección de datos, como la minimización de datos, de manera eficaz e integrar las garantías necesarias en el tratamiento a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados». Véanse también las Directrices 4/2019 del CEPD sobre el artículo 25 sobre la protección de datos desde el diseño y por defecto, párrafo 13.

⁴¹ En consecuencia, el considerando 39 del RGPD establece que los datos personales solo deben tratarse si la finalidad del tratamiento no puede cumplirse razonablemente por otros medios.

⁴² *Latvijas Republikas Saeima* (C-439/19), apartado 98; Sentencia del Tribunal de Justicia de 11 de diciembre de 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (en lo sucesivo, «C-708/18 *M5A-ScaraA*»), párrafo 48.

⁴³ Directrices 4/2019 del CEPD sobre el artículo 25 Protección de datos desde el diseño y por defecto, párrafo 48.

⁴⁴ Directrices 4/2019 del CEPD sobre el artículo 25 Protección de datos desde el diseño y por defecto, párrafo 14.

⁴⁵ Directrices 5/2020 del EDBP sobre el consentimiento con arreglo al Reglamento 2016/679, párrafo 5.

32. En cuanto al principio de **necesidad**, el Comité considerará si el tratamiento propuesto es necesario para alcanzar el objetivo perseguido y si el mismo objetivo puede alcanzarse con la misma eficacia por otros medios menos intrusivos para los derechos y libertades fundamentales del interesado⁴⁶. Por lo que respecta al principio de **proporcionalidad**, el Comité evaluará si el impacto negativo en los derechos y libertades fundamentales de los interesados es proporcional a cualquier beneficio previsto. Si el beneficio es relativamente menor, es posible que dicho impacto no sea proporcionado⁴⁷.
33. En cualquier caso, aunque el Comité considere que uno de los supuestos analizados a continuación podría cumplir los requisitos de los artículos 5.1.e) y f), 25 y 32 del RGPD, corresponde al responsable del tratamiento en cada caso demostrarlo con elementos fácticos. Dicha demostración debe incluir la consideración de escenarios alternativos.

3.2 Sobre la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD

3.2.1 Escenario 1: almacenamiento de la plantilla biométrica inscrita solo en manos de la persona, para autenticación

34. En esta sección se examina la compatibilidad con el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD del almacenamiento de la plantilla biométrica de los pasajeros únicamente en manos de la persona, por ejemplo, en su dispositivo individual⁴⁸, bajo su control exclusivo⁴⁹, para su autenticación⁵⁰ (en adelante, «**Escenario 1**»). Esta sección también examina las garantías adecuadas para el Escenario 1, a la luz de los artículos 25 y 32 del RGPD.

Descripción del escenario

35. En el escenario 1, la plantilla biométrica inscrita de cada pasajero, que ha dado su consentimiento para dicho tratamiento, solo se almacena en manos de la persona, por ejemplo, en un dispositivo individual mantenido por cada pasajero, bajo su control exclusivo. Los pasajeros son autenticados (comparación 1:1), cuando pasan por puntos de control específicos en el aeropuerto.
36. El registro del usuario en el sistema lo realiza el operador aeroportuario, ya sea de forma remota a través de la aplicación del operador aeroportuario⁵¹ o en las terminales aeroportuarias con el nivel de garantía de identidad adecuado (por ejemplo, el nivel de garantía adecuado de eIDAS⁵²). Dicho registro consiste en registrar, en el

⁴⁶Latvijas Republikas Saeima (C-439/19), apartados 110 y 113; Sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023, *Meta/Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, párrafo 108.

⁴⁷ M5A-ScaraA (C-708/18), apartados 52 a 56, Volker und Schecke (C-92/09 y C-93/09), apartado 87, Latvijas Republikas Saeima (C-439/19), apartados 98, 110 y 113. Véase también el artículo 29 del Dictamen 3/2012 del Grupo de Trabajo sobre tecnologías biométricas, p. 8.

⁴⁸ Como alternativa, la persona podría imprimir y almacenar su plantilla biométrica en papel.

⁴⁹ Esto se entiende sin perjuicio de la responsabilidad general del responsable del tratamiento en relación con el tratamiento.

⁵⁰ Como se ejemplifica en el caso de uso 1 del Anexo I de la solicitud.

⁵¹ El CEPD señala que en el futuro podrían contemplarse formas alternativas para dicha inscripción y que la inscripción podría llevarse a cabo sin la aplicación de un operador aeroportuario específico, por ejemplo, mediante la interacción con la cartera digital del usuario.

⁵² Un marco para la identificación electrónica y los servicios de confianza (en adelante, «eIDAS») basado en el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del Marco Europeo de Identidad Digital.

dispositivo del pasajero, una plantilla biométrica y los datos de identificación⁵³ (en adelante, "ID") necesarios para el tratamiento. El registro se realiza solo una vez y durante un período de validez específico (por ejemplo, alineado con el período de validez del pasaporte del pasajero). Ni el ID de los pasajeros ni sus datos biométricos son retenidos por el operador aeroportuario después del proceso de registro.

37. En particular, en lo que respecta al almacenamiento, la identificación y la plantilla biométrica del pasajero se almacenan localmente en el dispositivo de cada pasajero (por ejemplo, en la aplicación móvil del operador aeroportuario o en una aplicación de billetera digital). A continuación, el dispositivo puede utilizarse para transmitir o consultar el documento de identidad y la plantilla biométrica de los pasajeros, posiblemente incluyendo información de vuelo y/o la tarjeta de embarque. Por ejemplo, esta información puede estar encriptada con una clave que solo tenga el operador del aeropuerto, tal vez codificada en forma de código QR, que pueda imprimirse en papel o mostrarse en la pantalla del dispositivo del pasajero. En este caso, el pasajero mostraría este código QR en los puntos de control ubicados en el aeropuerto, equipados con un escáner QR y una cámara.
38. En términos de seguridad, durante el emparejamiento, los códigos QR se descifran con una clave en poder del operador del aeropuerto, que es el único capaz de descifrar los códigos QR. Los datos biométricos de los pasajeros se conservan solo durante un período muy corto y se eliminan después de que se complete la coincidencia. Cabe señalar que las medidas de seguridad en lo que respecta al almacenamiento dependen en parte de la seguridad del dispositivo del pasajero.

Evaluación del CEPD

39. El escenario 1 describe las medidas técnicas y organizativas diseñadas para garantizar un nivel de seguridad adecuado a los riesgos para los interesados, tal como se exige en los artículos 5, apartado 1, letra f), y 32 del RGPD. Los pasajeros son autenticados (comparación 1:1), cuando pasan por puntos de control específicos en el aeropuerto. En este escenario, la principal operación de coincidencia se realiza en el contexto de un entorno controlado⁵⁴, donde los pasajeros participan activamente y tienen más control sobre sus datos. En particular, solo se verificarían los pasajeros que dieran su consentimiento para dicho tratamiento y, dado que se verificarían en puntos de control específicos, no se recopilarían datos biométricos de otros pasajeros que no dieran su consentimiento para dicho tratamiento. Además, los pasajeros que dan su consentimiento tienen la posibilidad de detener el tratamiento en cualquier momento eliminando los datos de su dispositivo.
40. El uso del reconocimiento facial basado en una plantilla biométrica almacenada únicamente en manos de la persona, que puede estar, por ejemplo, en un dispositivo individual mantenido por el pasajero, bajo su exclusivo control, utilizado para la autenticación en puntos de control específicos a través de una interfaz dedicada, presenta, en determinadas condiciones, menos riesgos en comparación con el uso de datos biométricos en los que los datos se almacenan en una base de datos⁵⁵ centralizada. Este almacenamiento localizado, cuando va acompañado de las salvaguardias adecuadas⁵⁶, reduce la gravedad de las brechas de

⁵³ A los efectos del presente dictamen, los datos de identificación denotan datos, como el apellido, el nombre, la fecha de nacimiento, etc., que se ha verificado como exacto en relación con un documento de identidad o un pasaporte.

⁵⁴ El «entorno no controlado» se refiere al uso del reconocimiento facial para la identificación sin la participación activa de los interesados, en el que la plantilla de cada rostro que entra en la zona de vigilancia se compara con las plantillas de una amplia muestra representativa de la población almacenadas en una base de datos (véanse las Directrices 5/2022 del CEPD sobre el reconocimiento facial en las fuerzas y cuerpos de seguridad, párrafo 17).

⁵⁵ Directrices 5/2022 del CEPD sobre el reconocimiento facial en las fuerzas y cuerpos de seguridad, párrafo 17.

⁵⁶ Como se explica más adelante en el párrafo 46.

datos personales en comparación con el almacenamiento centralizado, en lo que respecta al número de personas afectadas, y garantiza que el acceso a la plantilla biométrica implicando la participación activa del interesado.

41. Además, el cotejo podría realizarse localmente en el aeropuerto, comparando la plantilla biométrica, por ejemplo contenida en el código QR, con la salida de la plantilla calculada en función de la muestra biométrica capturada por la cámara de la cápsula de control. Solo el resultado de la coincidencia se daría a conocer y sería utilizado por el responsable que realiza una verificación específica (que podría ser un operador aeroportuario o una compañía aérea, dependiendo de si se realiza en los puntos de control de seguridad del aeropuerto, la entrega de equipaje, el embarque y/o el acceso a la sala de pasajeros). Además, el hecho de que la información requerida para el cotejo (por ejemplo, el código QR) deba ser proporcionada por la persona actúa como un segundo factor y,⁵⁷ por lo tanto, refuerza la seguridad de la autenticación.
42. En cuanto a la compatibilidad con el artículo 25 del RGPD y, en particular, para cumplir con el requisito de minimización de datos, debe garantizarse que el tratamiento cumpla el principio de necesidad. En el escenario 1 podría considerarse que las medidas elegidas cumplen el principio de necesidad en relación con la finalidad perseguida (es decir, racionalizar el flujo de pasajeros) si, en función de las circunstancias del tratamiento, el responsable del tratamiento puede demostrar que no existen soluciones alternativas menos intrusivas que podrían alcanzar el mismo objetivo con la misma eficacia. Por ejemplo, el responsable puede demostrar que, incluso si los pasajeros tuvieran que mostrar su dispositivo, el escenario 1 acelera el proceso de verificación en comparación con la situación actual, ya que incluye a un humano que verifica si el nombre en la tarjeta de embarque coincide con el documento de identidad del pasajero⁵⁸. En particular, esto no pudo demostrarse si actualmente no se realizan controles para verificar la identidad de los pasajeros sobre la base de su documento oficial de identidad (a este respecto, véase el párrafo 18 *supra*).
43. Además, el operador aeroportuario no conserva las plantillas biométricas después de la inscripción y el período de conservación de los datos biométricos por parte del responsable que realiza la verificación es muy corto, ya que dichos datos se eliminan tan pronto como se completa la coincidencia. Por lo tanto, las medidas elegidas en el escenario 1 parecen limitar el alcance del tratamiento y el período de almacenamiento de los datos personales.
44. Por lo que respecta al principio de proporcionalidad, el carácter intrusivo de dicho tratamiento puede contrarrestarse con la participación activa de los pasajeros, ya que sus datos biométricos se almacenarían únicamente en sus manos. Además, teniendo en cuenta las medidas descritas anteriormente y suponiendo que el responsable del tratamiento aplique las salvaguardias adecuadas exigidas por el tratamiento específico en cuestión, la aplicación de las medidas adecuadas podría garantizar un nivel de seguridad adecuado al riesgo. En ese caso, el impacto negativo en los derechos y libertades fundamentales de los interesados podría considerarse proporcional al beneficio previsto.
45. Por lo tanto, teniendo en cuenta lo anterior, en respuesta a la pregunta 1.1, el Comité concluye que dicho tratamiento **podría considerarse en principio compatible con los artículos 5, apartado 1, letra f), 25 y 32 del RGPD, con sujeción a las garantías adecuadas.**

⁵⁷ Por ejemplo, esto mitiga el riesgo de suplantación de identidad. Véase también la salvaguardia C.1.2 *infra*.

⁵⁸ También se podría argumentar que la verificación biométrica puede ser menos propensa a errores que en comparación con una verificación humana.

Salvaguardias apropiadas

46. En este tipo de escenarios, en respuesta a la pregunta 1.2, el CEPD considera que deben aplicarse al menos las siguientes salvaguardias. *Podrían utilizarse otras salvaguardias distintas de las descritas en el presente dictamen para alcanzar los mismos objetivos de seguridad y protección de datos, y podrían ser lícitas siempre que garanticen el cumplimiento del marco jurídico aplicable.*
47. *Nota: esta es una descripción general de alto nivel y no exhaustiva de las posibles salvaguardas apropiadas, que debe implementar un responsable en una solución similar al Escenario 1. Su idoneidad en virtud de Los artículos 25 y 32 del RGPD dependerán de un análisis caso por caso. Todos los responsables deberán asegurarse de que llevan a cabo su propia evaluación de impacto de la protección de datos (en lo sucesivo, «EIPD»)⁵⁹ y sus soluciones específicas pueden requerir medidas adicionales no incluidas en el presente dictamen.*

A. General

A.1 Evaluación de impacto del tratamiento de datos

A.1.1 Llevar a cabo una EIPD, de conformidad con los requisitos del artículo 35 del RGPD, siempre que el responsable del tratamiento planifique una nueva operación de tratamiento que implique un tratamiento que pueda dar lugar a un alto riesgo. Es probable que este sea el caso del Escenario 1, ya que implica el tratamiento de datos biométricos a gran escala⁶⁰. Evaluar la idoneidad de implementar un sistema de reconocimiento facial, incluida su necesidad y proporcionalidad en relación con los fines perseguidos⁶¹, durante la fase inicial de diseño y revisarlo a lo largo del ciclo de vida del desarrollo del producto;

A.1.2 Consultar a la autoridad de control pertinente en caso de que el tratamiento siga entrañando un alto riesgo a pesar de las medidas adoptadas por el responsable del tratamiento para mitigar el riesgo⁶².

A.2 Derechos de los interesados y garantías que pueden implementar los responsables del tratamiento

A.2.1 Medidas de seguridad para abordar los casos de falsos negativos. Mitigar el riesgo de sesgo de edad, género y raza "evaluando regularmente si los algoritmos funcionan de acuerdo con los propósitos y ajustando los algoritmos para mitigar los sesgos descubiertos y garantizar la equidad en el tratamiento".⁶³ Por ejemplo, mediante la aplicación de la supervisión y la intervención humanas, con el fin de mitigar cualquier sesgo y garantizar que no se estigmatice ni se elabore un perfil de los pasajeros;

A.2.2 Garantizar que todo el tratamiento de datos personales sea transparente y que las personas sean conscientes y tengan el control de cómo se tratan sus datos en cada operación de tratamiento⁶⁴;

⁵⁹ Artículo 35 del RGPD.

⁶⁰ Artículo 35, apartado 3, del RGPD y Directrices del WP29 sobre la evaluación de impacto de la protección de datos (EIPD) y la determinación de si el tratamiento es «susceptible de dar lugar a un alto riesgo» a efectos del Reglamento 2016/679, adoptado el 13 de octubre de 2017, WP248rev.01, aprobado por el CEPD.

⁶¹ Artículo 35, apartado 7, letra b) del RGPD.

⁶² Artículo 36, apartado 1, del RGPD.

⁶³ Directrices 4/2019 del CEPD sobre el artículo 25 de la protección de datos desde el diseño y por defecto, nota a pie de página 60, párrafo 70.

⁶⁴ Directrices 4/2019 del CEPD sobre el artículo 25 de la protección de datos desde el diseño y por defecto, párrafo 68 y considerando 7 del RGPD.

A.2.3 Garantizar que se implementen medidas para cumplir con el principio de limitación de la finalidad, de modo que los datos no se utilicen para otros fines, como fines de seguridad o formación;

A.2.4 Asegurarse de que no se capturen fotos o vídeos, incluso si no se graban ni procesan, de personas que no den su consentimiento para el reconocimiento facial a través de medidas adecuadas (como el uso de una profundidad de campo y un área de captura adecuados para evitar la captura de imágenes de otros pasajeros en segundo plano o alrededor, el despliegue de colas dedicadas claramente etiquetadas para el reconocimiento facial);

A.2.5 Cuando los mismos puntos de control puedan ser utilizados por pasajeros que den su consentimiento y pasajeros que no den su consentimiento al reconocimiento facial, o cuando los pasajeros que no den su consentimiento al reconocimiento facial puedan aparecer en el campo de visión mientras el sistema no esté utilizado, el punto de control deberá esperar a que un pasajero que dé su consentimiento realizando una acción positiva antes de iniciar la captura de fotos o vídeos;

A.2.6 Posibilidad de que un interesado, en cualquier momento, realice la eliminación de los datos que están únicamente en sus manos (plantilla biométrica⁶⁵) que se encuentran en una aplicación móvil o cartera digital⁶⁶ ;

A.2.7 Existencia de alternativas viables o soluciones de respaldo (es decir, para los pasajeros que no consientan el uso de sus datos biométricos, para los pasajeros que no puedan utilizar dichas soluciones o para los pasajeros que sufran falsos rechazos) a fin de garantizar también que los pasajeros que no den su consentimiento no experimenten ningún perjuicio.⁶⁷;

A.2.8 Si se utiliza una aplicación, debe diseñarse y configurarse cuidadosamente para no recopilar datos innecesarios y evitar el uso de kits de desarrollo de software ("SDK", por sus siglas en inglés) de terceros que recopilen datos para otros fines.

A.3 Responsabilidad activa

A.3.1 Evaluar si existen códigos de conducta o mecanismos de certificación pertinentes que ayuden a demostrar el cumplimiento de la seguridad del tratamiento en el artículo 32 del RGPD⁶⁸. Verificar la idoneidad de las medidas para el tratamiento concreto de que se trate. Las normas⁶⁹, las mejores prácticas y los códigos de conducta, reconocidos por las asociaciones y otros organismos que representan a las categorías de responsables del tratamiento, pueden ser útiles para determinar las medidas adecuadas;

A.3.2 Garantizar que se realicen comprobaciones básicas de seguridad en el dispositivo de los usuarios para permitir la fase de inscripción, aunque el pasajero también tenga un papel en la protección de sus datos, ya que estos se almacenan en su dispositivo. Se presentan ejemplos de dichas comprobaciones y controles técnicos en la sección C.2 "Infraestructura y red".

⁶⁵ Las referencias a la plantilla biométrica en las medidas de seguridad del escenario 1 corresponden a las referencias a la clave/secreto en el escenario 2.

⁶⁶ Tenga en cuenta que esta protección solo se aplica al Escenario 1.

⁶⁷ Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 86.

⁶⁸ Artículo 32, apartado 3, del RGPD y Directrices 4/2019 del CEPD sobre el artículo 25 Protección de datos desde el diseño y por defecto, párrafo 10.

⁶⁹ Véase, por ejemplo, ISO/IEC 2382-37.

B. Organizativas:

B.1 Política y cumplimiento

B.1.1 Asegurarse de que los controles de acceso internos estén implementados⁷⁰ con reglas para los administradores;

B.1.2 Cuando el servicio de reconocimiento facial pueda ser prestado por una de las partes implicadas en el tratamiento sin datos identificativos o biométricos, o de ambos tipos, que deban ser tratados por las otras partes implicadas, prohibir que dichos datos fluyan a través de esas otras partes. Por ejemplo, una compañía aérea no necesita acceder técnicamente a los datos biométricos cuando depende de la infraestructura común del aeropuerto, incluso si esta compañía aérea actúa como responsable del tratamiento en virtud del RGPD;

B.1.3 Definir una política para el cifrado y la administración⁷¹ de claves, por ejemplo para el tratamiento de datos biométricos y de identificación;

B.1.4 Garantizar el cumplimiento del Capítulo V del RGPD. Por ejemplo, para garantizar transferencias conformes si el responsable del tratamiento utiliza un servicio a distancia durante el proceso de inscripción que tenga su sede en un tercer país;

B.1.5 Cuando se utilicen encargados del tratamiento, asegurarse de que existe un acuerdo de encargado del tratamiento⁷² de conformidad con el artículo 28, apartado 3, del RGPD;

B.1.6 Garantizar que existan procedimientos para gestionar la supervisión y la intervención humanas, en particular para hacer frente a los problemas de falso rechazo y a los problemas técnicos o de usabilidad.

B.2 Entrenamiento y pruebas

B.2.1 Asegurarse de que el personal esté capacitado de la manera adecuada;

B.2.2 Implementar un "proceso para probar, verificar y evaluar regularmente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento"⁷³;

B.2.3 Implementar un proceso para garantizar que el tratamiento de la plantilla⁷⁴ biométrica del pasajero para la autenticación sea técnicamente eficaz y suficientemente preciso;

B.2.4 Asegurarse de que las muestras biométricas recogidas tanto en el momento de la inscripción como en el punto de control sean de calidad suficiente para realizar un tratamiento biométrico fiable.

⁷⁰ Directrices 04/2020 del CEPD sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto del brote de COVID-19, adoptadas el 21 de abril de 2020 (en lo sucesivo, «**Directrices 4/2020 del CEPD sobre datos de localización y herramientas de rastreo de contactos**»), SEC-10, p. 16.

⁷¹ Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 89.

⁷² Artículo 28, apartado 3, del RGPD.

⁷³ Artículo 32, apartado 1, letra d) del RGPD.

⁷⁴ Las referencias a la plantilla biométrica en las salvaguardas para el escenario 1 corresponden a referencias a la clave/secreto en el escenario 2.

C. Técnicas:

C.1 Acceso

C.1.1 Aplicar salvaguardas durante la fase de inscripción para asegurar el inicio del proceso de inscripción con una identidad verificada. Por ejemplo, autenticación multifactor para reforzar la evaluación de las identidades de los usuarios, donde se pueden implementar por fases, que van desde enlaces de un solo uso protegidos con contraseña para activar la aplicación, hasta mecanismos de desbloqueo de dispositivos locales;

C.1.2 Implementar salvaguardas para abordar los casos de falsos positivos, ataques de suplantación de identidad biométrica y prevención de fraudes⁷⁵;

C.1.3 Prohibir cualquier acceso externo a la identificación y a los datos biométricos⁷⁶;

C.1.4 Garantizar que el tratamiento se realice localmente en las fases de inscripción, transmisión y emparejamiento. El punto de coincidencia debe estar lo más cerca posible del dispositivo de la persona. Habilitar la coincidencia de plantillas dentro del dispositivo individual puede requerir la interacción con proveedores de servicios ubicados fuera del aeropuerto y que impliquen el uso de recursos de red pública, con el inconveniente de afectar la disponibilidad y difundir la plantilla a entidades externas;

C.1.5 Autenticar a un usuario para agregar un nuevo vuelo y generar un nuevo código QR cifrado;

C.1.6 Implementar medidas para abordar la situación en la que un pasajero puede perder el acceso a su código QR.

C.2 Infraestructura y red

C.2.1 Condiciones sobre el sistema operativo ("SO") actualizado y la autenticación habilitada para el acceso al dispositivo para que la aplicación/cartera digital funcione, incluida la eliminación automática de datos biométricos y de identificación si el sistema operativo está desactualizado y plantea riesgos de seguridad;

C.2.2 Aislar las unidades correspondientes (es decir, puntos de control) de la red cuando estén en funcionamiento y tomar todas las demás medidas necesarias para garantizar la seguridad;

C.2.3 Realizar coincidencias biométricas en el dispositivo del pasajero o en el punto de control (*edge computing*);

C.2.4 Soluciones para abordar las vulnerabilidades de seguridad de los dispositivos individuales de los pasajeros, incluido el cifrado de (como mínimo) datos biométricos y de identificación almacenados;

⁷⁵ Informe de ENISA sobre Identidad Digital sobre el aprovechamiento del concepto de identidad autosoberana (SSI) para generar confianza, de enero de 2022.

⁷⁶ Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 89.

C.2.5 Utilizar un almacenamiento seguro para (al menos) datos biométricos únicamente a mano del usuario⁷⁷, por ejemplo, mediante el uso de un enclave seguro en un teléfono inteligente;

C.2.6 Salvaguardas de seguridad para garantizar la seguridad física de las instalaciones, incluida la terminal biométrica del aeropuerto. Garantizar un alto nivel de seguridad para los elementos de la arquitectura que procesan (por ejemplo, computación, flujo de datos, almacenamiento temporal o a largo plazo) datos biométricos y de identificación.

C.3 Seguridad y gestión de los datos de verificación de la identidad de los usuarios

C.3.1 Compartimentar los datos durante la transmisión y el almacenamiento en al menos tres grupos diferentes, tales como: identificación, datos biométricos y detalles de vuelo⁷⁸. Asegúrese de que los datos estén debidamente encriptados entre la transmisión y el almacenamiento;

C.3.2 Establecer medidas técnicas para garantizar que solo los datos que pueden procesarse legalmente en puntos de control específicos se procesen y verifiquen en el punto de control;

C.3.3 Garantizar la eficacia de la eliminación de datos⁷⁹ a través de un procedimiento de eliminación segura (por ejemplo, memoria principal, caché, posibles copias de seguridad) y evaluar cuándo debe automatizarse la eliminación de los datos. Los períodos de almacenamiento de datos deben aplicarse estrictamente a través de rutinas automáticas sin necesidad de una acción adicional por parte del individuo⁸⁰;

C.3.4 Garantizar la autenticidad e integridad de los datos (por ejemplo, la firma);⁸¹

C.3.5 Conservar los datos biométricos de los pasajeros en el punto de inscripción y en el punto de control solo durante un período muy breve y eliminarlos tan pronto como el pasajero haya pasado por el punto de control;

C.3.6 Si se utiliza una aplicación para el registro del usuario en el sistema, aplicar estándares de seguridad para la seguridad de la aplicación móvil durante el desarrollo de la aplicación, así como pruebas de seguridad por parte de un tercero;

C.3.7 Garantizar la aplicación de medidas de seguridad durante la fase de registro en el aeropuerto para preservar la confidencialidad e integridad de los datos biométricos del pasajero. Por ejemplo, si el quiosco imprime el código QR, el código QR no debe mostrarse en el quiosco para evitar que un actor malintencionado tome una foto. En los casos de transmisión a corta distancia, la transmisión debe realizarse basándose en la participación activa del usuario y a través de un canal que garantice la proximidad;

⁷⁷ Las referencias a la plantilla biométrica en las salvaguardas para el Escenario 1 corresponden a referencias a la clave/secreto en el escenario 2.

⁷⁸ Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 89.

⁷⁹ Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 89.

⁸⁰ Directrices 4/2019 del CEPD sobre el artículo 25 Protección de datos desde el diseño y por defecto, párrafo 82.

⁸¹ Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 89.

C.3.8 Los datos que están únicamente en manos de la persona⁸² deben guardarse en un almacenamiento seguro en el dispositivo de la persona y cualquier posible vulnerabilidad relacionada con los sistemas operativos del dispositivo debe someterse a los parches de seguridad adecuados. En el caso de un código QR impreso, la persona debe ser consciente de la naturaleza sensible particular de los datos que contiene y de lo que permite realizar;

C.3.9 Asegurarse de que la inscripción se realice siguiendo técnicas adecuadas de verificación de identidad remota⁸³.

3.2.2 Escenario 2: almacenamiento centralizado de la plantilla biométrica inscrita de forma cifrada dentro del aeropuerto y con una llave/secreto únicamente en manos de los pasajeros para su autenticación

48. En esta sección se examina la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD del almacenamiento centralizado, para la autenticación, de las plantillas biométricas inscritas de los pasajeros en una base de datos centralizada, de forma cifrada y con una clave/secreto que se mantenga únicamente en manos del pasajero⁸⁴ (en lo sucesivo, «**Escenario 2**»). En esta sección también se examinan las garantías adecuadas para el escenario 2, a la luz de los artículos 25 y 32 del RGPD.

Descripción del escenario

49. En el escenario 2 la inscripción se realiza una sola vez, durante un período de validez determinado (por ejemplo, un año después del último vuelo, hasta la expiración de la validez del pasaporte), ya sea de forma remota con el nivel de garantía de identidad adecuado (por ejemplo, el nivel de garantía adecuado de eIDAS) o en las terminales de los aeropuertos. La inscripción es controlada por el operador aeroportuario y consiste en la generación de datos identificativos y biométricos que se cifran con una clave/secreto.
50. La base de datos se almacena dentro de las instalaciones del aeropuerto, bajo el control del operador aeroportuario. Las claves/secretos de cifrado específicos de cada persona solo se almacenan en el dispositivo de la persona (por ejemplo, en la aplicación móvil del operador aeroportuario). La aplicación puede generar un código QR que contiene la clave/secreto, que puede imprimirse en papel o mostrarse en la pantalla del dispositivo⁸⁵. Además, el operador aeroportuario realiza una segunda capa de encriptación⁸⁶ con claves controladas por el operador aeroportuario.
51. Los pasajeros son autenticados (comparación 1:1), cuando pasan por puntos de control específicos en el aeropuerto. Los pasajeros que eligen pasar por los puntos de control biométricos muestran su código QR a un módulo de control dedicado equipado con un escáner QR y una cámara. El índice del pasajero se envía a la base de datos para solicitar la plantilla cifrada que se descarga y verifica localmente en el módulo de control

⁸² Las referencias a la plantilla biométrica en las salvaguardas para el escenario 1 corresponden a referencias a la clave/secreto.

⁸³ Véase el informe de ENISA sobre la verificación remota de la identidad: análisis de los métodos para llevar a cabo la verificación de la identidad a distancia, marzo de 2021.

⁸⁴ Como se ejemplifica en el caso de uso 2 del Anexo I de la Solicitud.

⁸⁵ FR SA ha aclarado además que también podría haber otras soluciones técnicas para enviar la información requerida, como el uso de un protocolo de comunicación de corto alcance.

⁸⁶ La clave/secreto (en manos del individuo) está encriptada con otra clave en poder del operador aeroportuario.

y/o dispositivo del usuario. Sólo el resultado coincidente es conocido y utilizado por el responsable de punto de control⁸⁷.

52. En este escenario, no hay flujos de datos biométricos y de identificación entre aeropuertos, sin interconexión ni interoperabilidad entre las bases de datos centralizadas.

Evaluación del CEPD

53. En el escenario 2 las plantillas biométricas inscritas de los pasajeros se almacenan de forma centralizada, pero de forma encriptada y con una clave/secreto únicamente en manos de los pasajeros. En el escenario 2 los pasajeros se autentican (comparación 1:1).
54. En este escenario, se propone que el objetivo de racionalizar el flujo de pasajeros (es decir, aumentando la velocidad de los controles) podría lograrse con el uso de un sistema centralizado. El CEPD ha señalado anteriormente que dicha solución podría considerarse una alternativa viable al almacenamiento descentralizado de las plantillas biométricas inscritas⁸⁸ (como se describe en el Escenario 1), si se presentan necesidades objetivas y con el uso de las salvaguardias adecuadas (véanse las salvaguardias descritas en el párrafo 60 *infra*).
55. En términos de consideraciones de seguridad, los datos de cada individuo están encriptados con la clave específica que solo mantiene el individuo y bajo su control exclusivo. Además, el hecho de que la información requerida para el cotejo (es decir, el secreto/clave) deba ser proporcionada por el individuo actúa como un segundo factor y,⁸⁹ por lo tanto, refuerza la seguridad de la autenticación. Además, el operador aeroportuario realiza una segunda capa de encriptación con claves controladas por el operador aeroportuario. En el escenario 2, el índice del individuo se envía a la base de datos central para recuperar los datos biométricos asociados con el individuo. A continuación, estos datos se envían (cifrados) a un ordenador localizado en el punto de control donde se descifran para realizar la coincidencia y solo el resultado de la coincidencia es conocido y utilizado por el responsable del punto de control. Siempre que la clave/secreto de la persona se guarde en el ordenador localizado en el punto de control y que solo se envíe el índice de un pasajero a la base de datos central para recuperar la plantilla biométrica cifrada, tales medidas de seguridad podrían considerarse compatibles con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD.
56. En cuanto a la compatibilidad con el artículo 25 del RGPD, y en particular para cumplir con el requisito de minimización de datos, debe garantizarse que el tratamiento cumpla el principio de necesidad. En el escenario 2, podría considerarse que las medidas elegidas cumplen el principio de necesidad en relación con la finalidad perseguida (es decir, racionalizar el flujo de pasajeros en los aeropuertos) si, en función de las circunstancias del tratamiento, el responsable del tratamiento puede demostrar que no existen soluciones alternativas menos intrusivas que podrían alcanzar el mismo objetivo con la misma eficacia. En el escenario 2, los pasajeros aún tendrían que mostrar su dispositivo⁹⁰. No obstante, el responsable del tratamiento puede demostrar que el

⁸⁷ La CA FR precisó que este período de conservación es ilustrativo y puede considerarse aceptable, dado que la clave está en manos de los particulares y puede elegirse en la fase de matriculación. Sin embargo, debe tenerse en cuenta que dicho período de almacenamiento puede ajustarse.

⁸⁸ Directrices 3/2019 del CEPD sobre dispositivos de vídeo, párrafo 88.

⁸⁹ Por ejemplo, esto mitiga el riesgo de suplantación de identidad. Véase también la salvaguarda C.1.2.

⁹⁰ La CA FR ha aclarado además que también podría haber otras opciones para presentar una plantilla, por ejemplo, impresa en papel. Además, el CEPD reconoce que en el futuro podría contemplarse el uso de una tecnología alternativa, p. ej. basado en un sistema de comunicación de campo cercano.

escenario 2 acelera el proceso de verificación en comparación con la situación actual, que incluye que un humano compruebe si el nombre que figura en la tarjeta de embarque coincide con el documento de identidad del pasajero⁹¹ o si se compara con el escenario 1. En particular, esto no pudo demostrarse si actualmente no se realizan controles para verificar la identidad de los pasajeros sobre la base de su documento oficial de identidad (a este respecto, véase el apartado 18 *supra*).

57. Por lo que respecta al principio de proporcionalidad, el carácter intrusivo de dicho tratamiento puede verse contrarrestado por la participación activa de los pasajeros, que tienen bajo su control exclusivo la clave de sus datos cifrados. Por otra parte, parece que los riesgos para la seguridad derivados del almacenamiento de los datos biométricos de los pasajeros en una base de datos centralizada y con la llave únicamente en manos de los pasajeros pueden mitigarse mediante el uso de garantías adecuadas (véanse las salvaguardias abordadas en el párrafo 60 *infra*). Por lo tanto, suponiendo que el responsable del tratamiento aplique las garantías adecuadas exigidas por el tratamiento específico en cuestión, los riesgos para las personas podrían mitigarse y el impacto negativo en los derechos y libertades fundamentales de los interesados podría considerarse proporcional al beneficio previsto. Por supuesto, en cada caso debe garantizarse que solo se procesen los datos necesarios para el propósito y que solo se verifiquen los pasajeros que dieron su consentimiento, por lo que no existe riesgo de que se recopilen datos biométricos de otros pasajeros que no dieron su consentimiento.
58. En la solicitud, se indica a modo de ejemplo que, en el escenario 2, el período de almacenamiento de los datos cifrados en la base de datos podría ser típicamente de un año después del último vuelo realizado por la persona y hasta el vencimiento de la validez del pasaporte. En la solicitud no se ha facilitado ninguna información que justifique un período tan largo sobre la base de razones objetivas, aunque cabe presumir que dicho período de conservación está previsto por motivos de conveniencia para vuelos futuros. En cuanto al período de almacenamiento, para lograr la compatibilidad con el artículo 5, apartado 1, letra e) del RGPD en este escenario, los responsables del tratamiento deben poder justificar por qué este período de conservación es necesario para ese fin en casos específicos. El Comité recomienda a los responsables del tratamiento que prevean el período de almacenamiento más breve posible, teniendo en cuenta también a los pasajeros que vuelan muy raramente, y ofrezca a los interesados que establezcan su período de almacenamiento preferido.
59. A la luz de estas consideraciones, en respuesta a la pregunta 2.1.1, el Comité concluye que dicho tratamiento **podría considerarse en principio compatible con los artículos 5, apartado 1, letras e), y f), 25 y 32 del RGPD, con sujeción a las garantías adecuadas.**

Salvaguardias apropiadas

60. En este tipo de escenario, en respuesta a la pregunta 2.1.2, el Comité considera que, además de **las salvaguardias enumeradas en el Escenario 1**, deben aplicarse al menos las siguientes salvaguardas. *Podrían utilizarse otras salvaguardias distintas de las descritas en el presente dictamen para alcanzar los mismos objetivos de seguridad y protección de datos, y podrían ser lícitas siempre que garanticen el cumplimiento de los marcos jurídicos aplicables.*
61. *Nota: esta es una descripción general de alto nivel y no exhaustiva de las posibles salvaguardas apropiadas, que podrían ser implementadas por un responsable en una solución similar al Escenario 2. Su idoneidad en virtud de los artículos 25 y 32 del RGPD dependerá de un análisis caso por caso. Todos los responsables del*

⁹¹ También se podría argumentar que la verificación biométrica puede ser menos propensa a errores que en comparación con una verificación humana.

tratamiento deberán asegurarse de llevar a cabo su propia EIPD y sus soluciones específicas pueden requerir medidas adicionales no incluidas en el presente dictamen.

D. General

D.1 Derechos de los interesados y garantías que pueden implementar los responsables del tratamiento

D.1.1 Asegurar de que el pasajero tenga control sobre los períodos de almacenamiento de datos para todos sus datos. Los períodos de almacenamiento deben limitarse a lo necesario para el propósito específico. Debe fijarse un plazo máximo como resultado de un análisis exhaustivo de factores como la validez del documento de identificación. Se debe ofrecer a los interesados la posibilidad de establecer su período de almacenamiento preferido, que podría ser más corto que el período de almacenamiento predeterminado;

D.1.2 Posibilidad de que un interesado solicite en cualquier momento la eliminación de los datos que están únicamente en sus manos (clave/secreto) que se encuentran en una aplicación móvil o billetera digital⁹²;

D.1.3 Garantizar que la localización de la base de datos central permita una supervisión eficaz por parte de la autoridad de control competente.

E. Organizativas

E.1 Políticas y cumplimiento

E.1.1 La confianza en el servidor central debe ser limitada. Asegurarse de que la gestión del servidor central siga reglas de gobernanza claramente definidas e incluya todas las medidas necesarias para garantizar su seguridad⁹³.

F. Técnicas:

F.1 Acceso

F.1.1 Mantener registros de quién tiene acceso a los datos personales, en particular los datos de identificación y biométricos, y cuándo se accedió a ellos;

F.2 Infraestructura y red

F.2.1 Proteger adecuadamente la base de datos central, incluso contra ataques de disponibilidad;

F.2.2 Asegurarse de que la base de datos central, los módulos de registro y los módulos de control no tengan conexión a Internet. La operación y el mantenimiento de estos sistemas (por ejemplo, copias de seguridad, parches, monitoreo, etc.) se realizarán localmente dentro de las instalaciones del aeropuerto.

F.3 Seguridad y gestión de datos

⁹² Tenga en cuenta que esta protección solo se aplica al Escenario 2.

⁹³ Directrices 4/2020 del CEPD sobre datos de localización y herramientas de rastreo de contactos, PRIV-5, p. 17.

F.3.1 Implementar técnicas criptográficas de última generación para asegurar los intercambios entre la aplicación y el servidor centralizado⁹⁴;

F.3.2 Mantener la clave/secreto individual en el nivel en el que se utilizará para descifrar (es decir, en el módulo de control) y utilizar el índice solo para recuperar la plantilla biométrica inscrita correspondiente en la base de datos central;

F.3.3 Asegurarse de que el intercambio de claves/secreto entre el dispositivo del usuario y el módulo de control proteja la comunicación contra cualquier posible espionaje o transmisión a terceros;

F.3.4 Indexar la plantilla biométrica cuando se almacene en la base de datos central para permitir la autenticación 1:1 y asegurarse de que sea única y esté relacionada con el individuo. Asegurarse de que el índice no revela ninguna información de identificación del pasajero y no está correlacionado con la clave de cifrado;

F.3.5 Autenticar y cifrar adecuadamente cualquier transmisión entre la base de datos central y los puntos de control e implementarla en redes aisladas;

F.3.6 Evitar los enlaces bidireccionales entre conjuntos de datos (datos de identificación y biométricos, así como detalles de vuelo) y mantener solo los enlaces unidireccionales relevantes en la base de datos. Por ejemplo, solo los vínculos unidireccionales del índice al ID, del índice a los datos biométricos cifrados y del índice a los detalles del vuelo;

F.3.7 Garantizar la continuidad de las actividades, por ejemplo, disponiendo de sistemas de almacenamiento de reserva adecuados;

F.3.8 Asegurarse de que el módulo de control (pod) no guarde registros de las plantillas cifradas o no cifradas.

3.2.3 Almacenamiento centralizado de las plantillas biométricas inscritas para su identificación

62. En esta sección se examina la compatibilidad con el artículo 5, apartado 1, letras e) y f), y los artículos 25 y 32 del RGPD del almacenamiento centralizado, para su identificación, de las plantillas biométricas inscritas de los pasajeros, cuando dichas plantillas no estén cifradas con una clave o secreto que se mantenga únicamente en manos de los pasajeros, en dos casos de uso: (1) cuando dichas plantillas se almacenen en una base de datos dentro del aeropuerto, bajo el control del operador aeroportuario⁹⁵ (en adelante, "**Escenario 3.1**"), y (2) cuando dichas plantillas se almacenen en la nube, bajo el control de la compañía aérea⁹⁶ (en adelante, "**Escenario 3.2**").
63. El Comité considera que el uso de datos biométricos con fines de **identificación** en grandes bases de datos centrales interfiere con los derechos fundamentales de los interesados y podría acarrear graves consecuencias

⁹⁴ Directrices 4/2020 del CEPD sobre datos de localización y herramientas de rastreo de contactos, SEC-4 p. 16: «Entre los ejemplos de técnicas que pueden utilizarse se incluyen, por ejemplo: cifrado simétrico y asimétrico, funciones hash, prueba de pertenencia privada, intersección de conjuntos privados, filtros de Bloom, recuperación de información privada, cifrado homomórfico».

⁹⁵ Como se ejemplifica en el caso de uso 3A del Anexo I de la solicitud.

⁹⁶ Como se ejemplifica en el caso de uso 3B del Anexo I de la solicitud.

para los interesados⁹⁷. Además, el uso de datos biométricos también debe examinarse en relación con la finalidad para la que se tratan, a la luz de los principios de necesidad y proporcionalidad⁹⁸.

3.2.3.1 Escenario 3.1: almacenamiento centralizado en una base de datos dentro del aeropuerto, bajo el control del operador aeroportuario

Descripción del escenario

64. En el escenario 3.1, la plantilla biométrica inscrita de los pasajeros se almacena en una base de datos central en las instalaciones del aeropuerto y bajo el control del operador aeroportuario de forma cifrada. En particular, los datos de los pasajeros están compartimentados, lo que significa que sus datos de identificación, la plantilla biométrica inscrita y la información de vuelo se almacenan en tres bases de datos diferentes. Dichos datos se cifran con diferentes claves, tanto durante el almacenamiento como durante la transmisión a los servidores que realizan la coincidencia, donde luego son descifrados por el operador aeroportuario.
65. Los pasajeros deben registrarse para cada vuelo, en un corto período de tiempo antes de su salida (por ejemplo, 48 horas). Dicha inscripción puede realizarse a distancia o en las terminales aeroportuarias con un nivel adecuado de garantía de identidad (por ejemplo, el nivel de garantía adecuado de eIDAS). Alternativamente, la inscripción puede tomar la misma forma que se describe en el Escenario 1, en cuyo caso los pasajeros deben enviar sus datos desde sus carteras digitales al sistema aeroportuario dentro de un plazo de 48 horas antes de su salida.
66. También en este escenario, los pasajeros se presentan en el módulo de control dedicado equipado con una cámara. A continuación, su muestra biométrica se envía a un servidor central del aeropuerto, que intentará hacer coincidir los datos con los de la base de datos biométrica central. De este modo, el pasajero puede ser identificado y comprobado si está registrado o no para un vuelo de salida (o para el vuelo de embarque en caso de control en el embarque). Dependiendo del punto de control, los datos enviados de vuelta al responsable del punto de control solicitante pueden minimizarse, por ejemplo, como una respuesta de "sí/no" o el propio resultado coincidente, si es necesario. En este caso, solo se transmite el resultado de la solicitud a un responsable de punto de control y se utiliza a este.
67. En particular, en este escenario se identifican los pasajeros (comparación 1:N), donde N es el número de pasajeros esperados en el aeropuerto en un período de tiempo de varios días. Además, el cotejo biométrico solo se realiza cuando cada pasajero se presenta en puntos de control predefinidos en el aeropuerto de salida, pero el tratamiento de datos en sí se realiza en un servidor central conectado a la base de datos central. El período de almacenamiento en este escenario suele ser de 48 horas y los datos se eliminan una vez que el avión ha despegado.

Evaluación del CEPD

68. Como se ha recordado anteriormente, el tratamiento de datos biométricos conlleva mayores riesgos para los derechos y libertades de los interesados⁹⁹. Por lo tanto, cualquier fallo en la seguridad de los datos puede tener

⁹⁷ Véase, por ejemplo, el artículo 29 del Dictamen 3/2012 del WP sobre tecnologías biométricas, p. 8. Véase también el párrafo 26 *supra*

⁹⁸ Considerando 4 del RGPD. Véase también el artículo 29 del Dictamen 3/2012 del Grupo de Trabajo sobre tecnologías biométricas, p. 8.

⁹⁹ Véase el párrafo 26 *supra*.

consecuencias especialmente graves para los interesados¹⁰⁰. Los responsables del tratamiento están obligados a mitigar eficazmente esos riesgos. Dado que en este escenario toda la arquitectura está completamente centralizada, los pasajeros pierden el control de sus datos en mayor medida. Además, el riesgo de que los datos acaben siendo tratados para otras finalidades distintas al control del flujo de pasajeros también podría ser mayor.

69. A la luz del principio y las exigencias de seguridad [artículo 5, apartado 1, letra f), y 32 del RGPD], debe considerarse que el almacenamiento de datos identificativos y biométricos en bases de datos centrales, aunque separadas, puede proporcionar puntos de ataque de gran valor y que una brecha de la confidencialidad de dicha base de datos puede implicar posteriormente el acceso a todo el conjunto de datos. En consecuencia, una posible brecha relativa a las plantillas de reconocimiento facial y a la identificación asociada puede permitir la identificación no autorizada o ilícita de los interesados en otros entornos. También puede, dependiendo de los métodos utilizados para la identificación biométrica, amenazar el uso seguro de las plantillas de reconocimiento facial como identificador. En ese caso, los efectos de la brecha no se pueden mitigar, a diferencia de lo que ocurre con otro tipo de credencial (por ejemplo, ID de usuario, contraseña) que son posibles de cambiar¹⁰¹.
70. Además, la gran cantidad y calidad de datos identificativos y biométricos en poder del responsable lo convierte en un objetivo muy valioso para un atacante, lo que conlleva, en términos de riesgo de seguridad, un mayor nivel de probabilidad. Además, las brechas de datos podrían tener un mayor impacto, ya que, debido al almacenamiento de datos en una ubicación centralizada, podría ser más fácil para los atacantes acceder a los datos personales relacionados con varios pasajeros. Por lo tanto, una posible brecha podría exponer a un gran número de interesados a altos riesgos en términos de gravedad, por ejemplo el robo de identidad a gran escala, que son extremadamente difíciles de mitigar.
71. Por lo tanto, en cuanto a la compatibilidad con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD, las medidas previstas en el escenario 3.1¹⁰², teniendo en cuenta el estado de la técnica, son insuficientes para garantizar un nivel de seguridad adecuado al riesgo. Sobre esta base, el tratamiento previsto en el escenario 3.1 no cumpliría con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD si un responsable del tratamiento se limitara a esas medidas.
72. A la luz del principio del artículo 5, apartado 1, letra e) del RGPD, en este escenario, el período de almacenamiento de datos biométricos en la base de datos central suele ser de 48 horas. Esta limitación de almacenamiento parece reducir significativamente los riesgos asociados a las brechas de datos personales. Sin embargo, el período de conservación de los datos no es un factor decisivo, por sí solo, para la compatibilidad global de dicha arquitectura, ya que dichos plazos de conservación pueden estar sujetos a cambios por parte de los responsables del tratamiento. En cualquier caso, las medidas propuestas deben cumplir los requisitos de protección de datos desde el diseño y por defecto en virtud del artículo 25 del RGPD.
73. A diferencia de los escenarios 1 y 2, en los que se autentica a los pasajeros, en el escenario 3.1 se identifica a los pasajeros (comparación 1:N), donde N es el número de pasajeros que se espera que lleguen al aeropuerto en un plazo de varios días y que hayan dado su consentimiento para dicho tratamiento al pasar por puntos de control específicos en el aeropuerto. Esto implica la búsqueda de pasajeros dentro de una base de datos

¹⁰⁰ Directrices sobre reconocimiento facial, Comité Consultivo del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos personales, junio de 2021, p. 22.

¹⁰¹ Véase, a este respecto, el Dictamen 3/2012 de A29WP sobre tecnologías biométricas, p. 34.

¹⁰² Como se ha descrito en los apartados 64 a 67 *supra*.

central, mediante el tratamiento de cada muestra biométrica capturada para comprobar si coincide con una persona conocida por el sistema. A diferencia del escenario 2, en el escenario 3.1, las claves/secretos no se mantienen únicamente en las manos de los pasajeros. En consecuencia, en este escenario, los pasajeros tienen mucho menos control sobre sus datos biométricos. Por lo tanto, dicho tratamiento como el propuesto en el escenario 3.1 no puede ser compatible con la protección de datos desde el diseño y los requisitos de diseño en virtud del artículo 25 del RGPD.

74. A la luz del artículo 25 del RGPD, los responsables del tratamiento deben tener en cuenta los tipos, las categorías y el nivel de detalle de los datos personales necesarios para los fines del tratamiento¹⁰³. Sus opciones de diseño deben tener en cuenta el aumento de los riesgos para los principios de minimización, integridad y confidencialidad de los datos, así como la limitación del almacenamiento, cuando se recopilan grandes cantidades de datos personales detallados, y compararlo con la reducción de los riesgos cuando se recopilan cantidades más pequeñas y/o información menos detallada sobre los interesados. En cualquier caso, la configuración predeterminada no debe incluir la recopilación de datos personales que no sean necesarios para el propósito específico del tratamiento. En otras palabras, si ciertas categorías de datos personales son innecesarias o si no se necesitan datos detallados porque los datos menos granulares son suficientes, entonces no se deben recopilar datos personales sobrantes. En este caso, si otra implementación de tratamiento podría lograr el mismo objetivo y está disponible según los términos descritos en el escenario 3.1, no es necesario utilizar la tecnología de reconocimiento facial.
75. En cuanto al artículo 25 del RGPD, un elemento clave de la protección de datos desde el diseño y por defecto es la autonomía del interesado. En particular, debe concederse al interesado el mayor grado de autonomía posible para determinar el uso que se hace de sus datos personales, así como sobre el alcance y las condiciones de dicho uso o tratamiento¹⁰⁴. En el Escenario 1, el interesado tendría autonomía y control con respecto al uso, la divulgación y el borrado de sus plantillas biométricas y, en el Escenario 2, el interesado mantendría cierto control con respecto a la divulgación de su propia plantilla biométrica, ya que su clave/secretos de cifrado se almacenaría en sus manos. Sin embargo, en el escenario 3.1, el interesado depende totalmente de las decisiones del responsable del tratamiento en relación con el tratamiento de sus datos biométricos y, por lo tanto, no tiene control directo sobre el uso de su plantilla biométrica.
76. En cuanto a la compatibilidad con el artículo 25 del RGPD, y en particular para cumplir con el requisito de minimización de datos, el tratamiento previsto en el escenario 3.1 no puede cumplir el principio de necesidad. El Comité considera que se puede lograr un resultado similar para racionalizar el flujo de pasajeros en los aeropuertos de una manera menos intrusiva en materia de privacidad. Por ejemplo, esto se puede lograr sin el uso de datos biométricos (aunque la experiencia del usuario sería diferente, ya que podría llevar más tiempo mostrar su tarjeta de embarque y, en su caso, los documentos de identificación oficiales). Además, otras soluciones, en particular las que se basan en el almacenamiento de los datos biométricos en una billetera local en el dispositivo de la persona o las que requieren el cifrado de los datos con una clave específica almacenada en el dispositivo de la persona, permiten alcanzar los objetivos de una manera menos intrusiva en cuanto a la privacidad.
77. En cuanto al principio de proporcionalidad, el tratamiento previsto en el escenario 3.1 crearía riesgos para los derechos de los interesados que no se verían mitigados por las medidas previstas dado el estado de la técnica.

¹⁰³ Directrices 4/2019 del CEPD sobre protección de datos desde el diseño y por defecto, párrafo 49.

¹⁰⁴ Directrices 4/2019 del CEPD sobre protección de datos desde el diseño y por defecto, apartado 70. El considerando 7 del RGPD aclara además que "las personas naturales deben tener el control de sus propios datos personales".

El riesgo de un impacto negativo en los derechos y libertades fundamentales de los interesados que podría derivarse de una brecha de datos en una base de datos centralizada de datos biométricos de un gran número de personas parece superar el beneficio previsto derivado del tratamiento, ya que dicho beneficio es relativamente menor, es decir, un ligero aumento de la comodidad y la rapidez de los controles. Por lo tanto, no puede justificar el elevado carácter intrusivo de estas medidas en favor de los derechos y libertades fundamentales de las personas y el tratamiento previsto en el supuesto 3.1 no cumple el principio de proporcionalidad.

78. A la luz de estas consideraciones, en respuesta a la pregunta 2.2.1, el Comité concluye que, cuando el tratamiento se realiza con el propósito específico de racionalizar el flujo de pasajeros en los aeropuertos, el tratamiento previsto en el escenario 3.1:
- **no puede ser compatible con el artículo 25 del RGPD;**
 - **no cumpliría con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD** si un responsable del tratamiento se limitara a las medidas descritas en el escenario 3.1.

3.2.3.2 Escenario 3.2: almacenamiento centralizado en una nube, bajo el control de la compañía aérea

Descripción del escenario

79. En el escenario 3.2, la plantilla biométrica inscrita de los pasajeros se almacena en la nube, bajo el control de la compañía aérea o su proveedor de servicios en la nube (encargado del tratamiento). En la solicitud, se especifica que el proveedor de servicios en la nube se ubicaría en el EEE¹⁰⁵. En este caso, los datos de los pasajeros están encriptados, pero descifrados cuando están en uso (por ejemplo, cuando se realiza la operación de cotejo o emparejamiento), y las claves son controladas por la compañía aérea o su encargado del tratamiento en la nube. Los datos biométricos de los pasajeros se utilizan para la identificación de los pasajeros (comparación 1:N), donde N es potencialmente hasta el número total de clientes de la compañía aérea¹⁰⁶.
80. Al igual que en los escenarios 1, 2 y 3.1, también en este caso los pasajeros deben registrarse previamente en el sistema. Sin embargo, en el escenario 3.2, el registro de los pasajeros se realiza una vez, mientras el cliente tenga una cuenta con la compañía aérea. La inscripción se realiza de forma remota con un nivel adecuado de garantía de identidad (por ejemplo, un nivel de garantía adecuado de eIDAS) o en las terminales de los aeropuertos. El cotejo biométrico solo se realiza cuando los pasajeros se presentan en puntos de control predefinidos en el aeropuerto, pero el tratamiento de datos en sí se realiza en la nube.
81. En el aeropuerto, los pasajeros pasan por puestos de control dedicados, equipados con una cámara. Los datos biométricos de los pasajeros se envían a través de una solicitud a un servidor en la nube de la aerolínea, donde se realiza el cotejo de estos datos con la base de datos central. De este modo, el pasajero puede ser identificado y comprobado si está registrado o no para un vuelo de salida (o para el vuelo de embarque en caso de control en el embarque).
82. Potencialmente, los resultados coincidentes pueden ponerse a disposición de múltiples operadores aeroportuarios cuando una compañía aérea tiene una terminal dedicada o acceso a la infraestructura del

¹⁰⁵ CA FR aclaró que esto es ilustrativo y que también podrían contemplarse proveedores de servicios en la nube que no estén ubicados en el EEE. Además, también podrían contemplarse otras soluciones de almacenamiento (por ejemplo, sin uso de la nube).

¹⁰⁶ CA FR aclaró que esto es ilustrativo y que existe una solución en la que los datos biométricos se envían cada vez antes del vuelo.

sistema de información común de un aeropuerto. Dependiendo del punto de control, los datos enviados de vuelta al responsable del punto de control solicitante pueden minimizarse, por ejemplo, como una respuesta de "sí/no" o el propio resultado coincidente, si es necesario. En este caso, solo el responsable de punto de control conoce y utiliza el resultado de la solicitud.

83. El período de almacenamiento de la plantilla lo define la compañía aérea y puede durar mientras el cliente tenga una cuenta en la compañía aérea.

Evaluación del CEPD

84. Las consideraciones ya expresadas por el Comité Directiva en relación con el Escenario 3.1¹⁰⁷ también se aplican a este Escenario.
85. En cuanto al principio y los requisitos de seguridad (artículos 5, apartado 1, letra f), y 32 del RGPD), el tratamiento del escenario 3.2 se realiza en la nube y varias entidades podrían tener acceso a dichos datos, entre ellos posiblemente proveedores no pertenecientes al EEE, incluso cuando los datos se conserven en el EEE¹⁰⁸. Dicha arquitectura conlleva riesgos potenciales en relación con las transferencias de datos personales a terceros países. Además, aunque los datos de los pasajeros están encriptados, se descifran cuando están en uso (es decir, cuando se realiza la operación de coincidencia), mientras que las claves son controladas por la compañía aérea o su encargado del tratamiento en la nube. Este almacenamiento puede dar lugar a un mayor aumento de las situaciones de exposición de seguridad.
86. Por lo tanto, en cuanto a la compatibilidad con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD, las medidas previstas en el escenario 3.2¹⁰⁹, teniendo en cuenta el estado de la técnica, son insuficientes para garantizar un nivel de seguridad adecuado al riesgo. Sobre esta base, el tratamiento previsto en el escenario 3.2 no cumpliría con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD si un responsable del tratamiento se limitara a esas medidas.
87. Además, de acuerdo con el escenario 3.2¹¹⁰, los datos podrían almacenarse durante un período significativo (p. ej. puede durar mientras el interesado tenga una cuenta en la compañía aérea). Dicha duración del almacenamiento expone a los datos a mayores riesgos de brechas de su confidencialidad e integridad y parece ir más allá de lo estrictamente necesario y proporcionado para los fines del tratamiento. El Comité observa que el período de almacenamiento de datos no es un factor decisivo, en sí mismo, para la compatibilidad general con el RGPD de dicha arquitectura, ya que puede estar sujeto a cambios por parte de los controladores de datos. Sin embargo, sobre la base de la información disponible para el Comité y contenida en la descripción del Escenario 3.2, no existe una justificación suficiente para este prolongado período de retención y no hay medidas aparentes para mitigar los riesgos para las personas. En base a esto, el período de almacenamiento propuesto no se limitaría a lo necesario, de conformidad con el principio de limitación de almacenamiento establecido en el artículo 5, apartado 1, letra e) del RGPD.
88. En cualquier caso, las medidas propuestas en el escenario 3.2 no pueden satisfacer los requisitos de protección de datos desde el diseño y por defecto del artículo 25 del RGPD. En el escenario 3.2, las plantillas biométricas inscritas de los pasajeros se almacenan en la nube, bajo el control de la compañía aérea o su proveedor de

¹⁰⁷ Párrafos 68 a 77 *supra*.

¹⁰⁸ CEPD 2022, Acción coordinada de ejecución sobre el uso de servicios basados en la nube por el sector público, de 17 de enero de 2023, p. 19.

¹⁰⁹ Véanse los párrafos 79 a 83 *supra*.

¹¹⁰ Véase el párrafo 83 *supra*.

servicios en la nube (encargado del tratamiento). Como se ha descrito anteriormente, varias entidades podrían tener acceso a estos datos. Además, los datos biométricos de los pasajeros se utilizan para la identificación de los pasajeros (comparación 1:N), donde N es potencialmente hasta el número total de usuarios/clientes de la compañía aérea. Este método consiste en encontrar a una persona entre un grupo de personas dentro de la base de datos central, procesando cada rostro capturado para comprobar si coincide con una persona conocida por el sistema. A diferencia del escenario 3.1, en el escenario 3.2 la comparación podría realizarse a una escala mucho mayor, ya que el criterio aquí es el número total de clientes de la compañía aérea, mientras que el escenario 3.1 solo incluía el número de pasajeros esperados en un período de varios días.

89. Además, en lo que respecta a la compatibilidad con el artículo 25 del RGPD y, en particular, para cumplir con el requisito de minimización de datos, el tratamiento previsto en el escenario 3.2 no puede cumplir el principio de necesidad. El Comité considera que se podría lograr un resultado similar para agilizar el flujo de pasajeros en los aeropuertos mediante otras medidas menos intrusivas, por ejemplo, sin el uso de datos biométricos, aunque la experiencia del usuario sería diferente, ya que podría llevar más tiempo mostrar su documento de identidad y su tarjeta de embarque. Además, otras soluciones, en particular las que se basan en el almacenamiento de los datos biométricos en una cartera digital local en el dispositivo de la persona o las que requieren el cifrado de los datos con una clave específica almacenada en el dispositivo de la persona, permiten al responsable del tratamiento alcanzar los objetivos de una manera menos intrusiva en materia de privacidad.
90. Por lo que respecta al principio de proporcionalidad, el tratamiento previsto en el escenario 3.2 crearía riesgos para los derechos de los interesados que no se verían mitigados por las salvaguardias previstas. El impacto negativo en los derechos y libertades fundamentales de los interesados que se derivaría de una brecha de datos en una base de datos centralizada de datos biométricos de un gran número de personas almacenados en la nube parece superar el beneficio previsto del tratamiento, ya que dicho beneficio es relativamente menor, es decir, un ligero aumento de la comodidad y la rapidez de los controles. Por lo tanto, no puede justificar el elevado carácter intrusivo de estas medidas para los derechos y libertades fundamentales de las personas y el tratamiento previsto en el supuesto 3.2 no puede considerarse proporcionado.
91. A la luz de estas consideraciones, en respuesta a la pregunta 2.3.1, el Comité concluye que, cuando el tratamiento se realiza con el propósito específico de racionalizar el flujo de pasajeros en los aeropuertos, el tratamiento previsto en el escenario 3.2:
- **no puede ser compatible con el artículo 25 del RGPD;**
 - **no cumpliría con el artículo 5, apartado 1, letra f), y el artículo 32 del RGPD** si un responsable del tratamiento se limitara a las medidas descritas en el escenario 3.2;
 - **no cumpliría con el artículo 5, apartado 1, letra e) del RGPD**, ya que no existe una justificación suficiente para el período de retención previsto en el escenario 3.2, sobre la base de la información de que dispone la Junta. Para cumplir con el principio de limitación de la conservación del artículo 5, apartado 1, letra e) del RGPD, el responsable del tratamiento tendría que demostrar que los datos personales no se conservan más tiempo del necesario para los fines para los que se tratan.

4 CONCLUSIONES

92. En relación con la pregunta 1.1, sobre la base de la solicitud de dictamen de FR SA, en relación con los requisitos de los artículos 5, apartado 1, letra f), 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:

93. el uso de la tecnología de reconocimiento facial para la autenticación basada en la biometría, con el fin específico de racionalizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros) podría considerarse en principio compatible con los principios de integridad y confidencialidad consagrados en el artículo 5, apartado 1, letra f), y en los artículos 25 y 32 del RGPD, en el caso de una arquitectura de almacenamiento, cuando la plantilla biométrica inscrita de cada pasajero se almacene localmente en su dispositivo individual y bajo su control exclusivo, si está sujeta a las salvaguardias adecuadas descritas en el párrafo 46 *supra*.
94. En relación con la cuestión 2.1.1, sobre la base de la solicitud de dictamen de la FR SA, en relación con los requisitos del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:
95. el uso de la tecnología de reconocimiento facial para la autenticación basada en la biometría, con el fin específico de racionalizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros) podría considerarse compatible en principio con el principio de limitación de almacenamiento establecido en el artículo 5, apartado 1, letra e), y con los principios de integridad y confidencialidad previstos en el artículo 5, apartado 1, letra f), y los artículos 25 y 32 del RGPD en el caso de una arquitectura de almacenamiento centralizado, en la que la plantilla biométrica inscrita de cada pasajero se almacena en una base de datos central dentro del aeropuerto, bajo el control del operador aeroportuario, de forma encriptada, con una clave/secreto en manos exclusivas de la persona, si está sujeta a las garantías adecuadas descritas en el apartado 60 *supra*.
96. En cuanto a la cuestión 2.2.1, sobre la base de la solicitud de dictamen de FR SA en relación con los requisitos del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:
97. el uso de tecnología de reconocimiento facial para la identificación basada en la biometría, utilizada con el fin específico de racionalizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros) en el caso de una arquitectura de almacenamiento centralizada, cuando las plantillas biométricas inscritas de los pasajeros no estén encriptadas con una clave o secreto que se mantenga únicamente en las manos de cada pasajero, cuando dichas plantillas se almacenen en una base de datos dentro del aeropuerto (bajo el control del operador aeroportuario), no pueden ser compatibles con el artículo 25 del RGPD. Además, dicho tratamiento no cumpliría con el principio de integridad y confidencialidad del artículo 5, apartado 1, letra f), y del artículo 32 del RGPD, si un responsable del tratamiento se limitara a las medidas descritas en el escenario 3.1.
98. En cuanto a la cuestión 2.3.1, sobre la base de la solicitud de dictamen de FR SA en relación con los requisitos del artículo 5, apartado 1, letras e) y f), y de los artículos 25 y 32 del RGPD, y sobre la base del análisis anterior, el Comité concluye que:
99. el uso de tecnología de reconocimiento facial para la identificación basada en la biometría, utilizada con el fin específico de racionalizar el flujo de pasajeros en los aeropuertos (controles de seguridad, entrega de equipajes, embarque y acceso a la sala de pasajeros) en el caso de una arquitectura de almacenamiento centralizada, cuando las plantillas biométricas inscritas de los pasajeros no estén encriptadas con una clave o secreto que se mantenga únicamente en las manos de cada pasajero, cuando dichas plantillas se almacenan en la nube (bajo el control de la compañía aérea) no pueden ser compatibles con el artículo 25 del RGPD. Además, dicho tratamiento no cumpliría los principios de integridad y confidencialidad establecidos en el artículo 5, apartado 1, letra f), y en el artículo 32 del RGPD, si un responsable del tratamiento se limitara a las

medidas descritas en el escenario 3.2. Por último, sobre la base de la descripción del escenario 3.2 y de la información de que dispone la Junta, el tratamiento no cumpliría el principio de limitación de almacenamiento previsto en el artículo 5, apartado 1, letra e) del RGPD.

El Comité Europeo de Protección de Datos

La Presidenta

(Anu Talus)