Parere del comitato (articolo 64)

Parere 11/2024 sull'uso del riconoscimento facciale per snellire il flusso dei passeggeri negli aeroporti (compatibilità con l'articolo 5, paragrafo 1, lettere e) e f), e gli articoli 25 e 32 GDPR)

Versione 1.1

Adottato il 23 maggio 2024

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

Adottato

Versione 1.1	28 maggio 2024	Correzione grammaticale nella sintesi (pagg. 3 e 4) e nei punti 77 e 90 del parere
Versione 1.0	23 maggio 2024	Adozione del parere

Sintesi

L'autorità di controllo francese ha chiesto al Comitato europeo per la protezione dei dati di emettere un parere sull'uso della tecnologia di riconoscimento facciale da parte dei gestori aeroportuali e delle compagnie aeree per l'autenticazione o l'identificazione biometrica dei passeggeri al fine di snellire il flusso di questi ultimi negli aeroporti.

Come osservazione preliminare, il Comitato ricorda che l'uso dei dati biometrici e in particolare della tecnologia di riconoscimento facciale comporta maggiori rischi per i diritti e le libertà degli interessati. Si tratta di un trattamento di dati biometrici cui è accordata una protezione particolare ai sensi dell'articolo 9 GDPR. Prima di utilizzare tali tecnologie, anche se dovessero essere ritenute particolarmente efficaci, i titolari del trattamento dovrebbero valutare l'impatto sui diritti e sulle libertà fondamentali degli interessati e considerare se mezzi meno invasivi possano raggiungere la finalità legittima del rispettivo trattamento.

L'ambito di applicazione del presente parere, come da richiesta, è limitato alla compatibilità del trattamento con **l'articolo 5, paragrafo 1, lettere e) e f)**, e con **gli articoli 25 e 32 GPDR** al **fine specifico di snellire il flusso dei passeggeri negli aeroporti** in quattro specifici punti di controllo, ossia i punti di controllo di sicurezza, la consegna dei bagagli, l'imbarco e l'accesso alla sala d'attesa per i passeggeri. Il presente parere non include un'analisi completa ed esaustiva della conformità al GDPR da parte del relativo titolare o dei relativi titolari del trattamento in ciascun caso, nonché del loro responsabile o dei loro responsabili del trattamento, se del caso. Pertanto il presente parere non pregiudica un'analisi giuridica e tecnica caso per caso basata sulle circostanze e sul trattamento specifici previsti da un titolare del trattamento. Inoltre l'analisi della base giuridica applicabile non rientra nell'ambito delle domande sottoposte al Comitato nella richiesta e di conseguenza la validità del consenso a tale trattamento, conformemente agli articoli 6, 7 e 9 GDPR, non è esaminata nella presente opinione. Inoltre il presente parere non pregiudica le limitazioni all'uso dei dati biometrici previste dal diritto degli Stati membri.

Nel presente parere il Comitato valuta la conformità del trattamento alle suddette disposizioni del GDPR nel contesto di **quattro scenari specifici**.

Il **primo scenario** prevede la conservazione di un modello biometrico registrato nelle mani della persona, ad esempio su un suo singolo dispositivo, sotto il suo esclusivo controllo, al fine di autenticare (confronto 1:1) il passeggero man mano che procede attraverso i suddetti punti di controllo aeroportuali.

Il Comitato conclude che le misure scelte potrebbero essere considerate conformi al principio di necessità se il titolare del trattamento può dimostrare che non esistono soluzioni alternative meno invasive in grado di conseguire lo stesso obiettivo in modo altrettanto efficace. Inoltre l'invasività del trattamento può essere controbilanciata dal coinvolgimento attivo dei passeggeri, in quanto il modello biometrico di questi ultimi è conservato solo nelle loro mani, ad esempio su un loro singolo dispositivo, sotto il loro esclusivo controllo e i loro dati sono cancellati poco dopo il completamento del confronto. Su tale base il Comitato conclude che il trattamento previsto nel primo scenario **potrebbe essere considerato in linea di principio compatibile con l'articolo 5, paragrafo 1, lettera f), e con gli articoli 25 e 32 GDPR**, fatta salva l'attuazione di garanzie adeguate.

Il Comitato ha individuato le garanzie che, come minimo, dovrebbero essere attuate per una soluzione simile al primo scenario.

Il **secondo scenario** prevede la conservazione centralizzata all'interno dell'aeroporto di un modello biometrico registrato in forma cifrata con una chiave segreta nota esclusivamente al passeggero. Ciò consente l'autenticazione dei passeggeri (confronto 1:1) man mano che procedono attraverso i suddetti punti di controllo aeroportuali. La registrazione è valida per un determinato periodo che ad esempio potrebbe arrivare fino a un anno dopo l'ultimo volo effettuato fino alla data di scadenza del passaporto.

Il Comitato conclude che il trattamento possa essere ritenuto conforme al principio di necessità se il titolare del trattamento può dimostrare che non esistono soluzioni alternative meno invasive in grado di conseguire lo stesso obiettivo in modo altrettanto efficace. Inoltre l'invasività del trattamento può essere controbilanciata dal coinvolgimento attivo del passeggero, che detiene sotto il suo esclusivo controllo la chiave segreta dei suoi dati biometrici cifrati. Se il titolare del trattamento attua garanzie adeguate, i rischi per la sicurezza derivanti dall'utilizzo di una banca dati centralizzata in questo scenario potrebbero essere attenuati e l'impatto negativo sui diritti e sulle libertà fondamentali degli interessati potrebbe essere considerato proporzionato al vantaggio previsto. Per quanto riguarda il principio della limitazione della conservazione, al Comitato non è stata fornita alcuna informazione a sostegno del lungo periodo di conservazione. Al fine di conseguire la compatibilità con l'articolo 5, paragrafo 1, lettera e), GDPR in questo scenario, i titolari del trattamento dovrebbero essere in grado di giustificare il motivo per cui il periodo di conservazione previsto è necessario per la finalità in casi specifici. Il Comitato raccomanda ai titolari del trattamento di prevedere un periodo di conservazione il più breve possibile, offrendo al contempo ai passeggeri la possibilità di stabilire il periodo di conservazione che preferiscono. Su tale base il Comitato conclude che il trattamento previsto nello scenario 2 **potrebbe essere considerato in linea di principio compatibile con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR**, fatta salva l'attuazione di garanzie adeguate.

Il Comitato ha individuato le garanzie che, come minimo, dovrebbero essere attuate per una soluzione simile al secondo scenario.

Il **terzo scenario** prevede la conservazione centralizzata di un modello biometrico registrato in forma cifrata all'interno dell'aeroporto sotto il controllo del gestore aeroportuale. Ciò consente l'identificazione dei passeggeri (confronto 1:N) man mano che procedono attraverso i suddetti punti di controllo aeroportuali. Il periodo di conservazione in questo scenario è generalmente di 48 ore e i dati sono cancellati al decollo dell'aereo.

Dal momento che la conservazione dei dati identificativi e biometrici avviene in una banca dati centrale, se la riservatezza di quest'ultima è compromessa, ciò può successivamente comportare l'accesso all'intero insieme di dati e consentire l'identificazione non autorizzata o illecita dei passeggeri in altri ambienti. L'architettura di conservazione centralizzata sotto il controllo del gestore aeroportuale comporta altresì che il passeggero perda maggiormente il controllo dei suoi dati. Il Comitato ritiene che un risultato analogo per quanto riguarda lo snellimento del flusso dei passeggeri negli aeroporti possa essere conseguito in modo meno invasivo e che l'impatto negativo sui diritti e sulle libertà fondamentali degli interessati che risulterebbe da una violazione dei dati in una banca dati centralizzata di dati biometrici sembra superare il vantaggio previsto derivante dal trattamento. Pertanto il trattamento non può soddisfare i principi di necessità e proporzionalità. Su tale base il Comitato conclude che il trattamento previsto nel terzo scenario **non può essere compatibile con l'articolo 25 GDPR**. Inoltre **non sarebbe conforme all'articolo 5, paragrafo 1), lettera f), e all'articolo 32 GDPR** se un titolare del trattamento si limitasse alle misure descritte in questo scenario.

Il **quarto scenario** prevede la conservazione centralizzata di un modello biometrico registrato in forma cifrata nel cloud sotto il controllo della compagnia aerea o del suo fornitore di servizi cloud. Ciò

consente l'identificazione dei passeggeri (confronto 1:N) man mano che procedono attraverso i suddetti punti di controllo aeroportuali. Il periodo di conservazione in questo scenario può potenzialmente durare fino a quando il cliente ha un account presso la compagnia aerea.

Dal momento che la conservazione dei dati identificativi e biometrici avviene in una banca dati centrale nel cloud, più soggetti potrebbero avere accesso a tali dati, compresi eventualmente fornitori di paesi non appartenenti al SEE. I dati del passeggero sono decifrati quando sono utilizzati e le chiavi sono sotto il controllo della compagnia aerea o dei suoi responsabili del trattamento, il che potrebbe aumentare la superficie di esposizione alla sicurezza. Tale architettura di conservazione centralizzata comporta altresì che il passeggero perda maggiormente il controllo dei suoi dati. I dati potrebbero anche essere conservati per un periodo di tempo significativo, il che li espone a rischi più elevati di violazione della sicurezza e sembra andare oltre quanto strettamente necessario e proporzionato ai fini del trattamento, a meno che non siano adottate ulteriori misure evidenti per attenuare i rischi per le persone.

Il Comitato ritiene che un risultato analogo per quanto riguarda lo snellimento del flusso dei passeggeri negli aeroporti possa essere conseguito in modo meno invasivo e che l'impatto negativo sui diritti e sulle libertà fondamentali degli interessati che potrebbe risultare da una violazione dei dati in una banca dati centralizzata di dati biometrici sembra superare il vantaggio previsto derivante dal trattamento. Pertanto il trattamento non può soddisfare i principi di necessità e proporzionalità. Su tale base il Comitato conclude che il trattamento previsto nel quarto scenario **non può essere compatibile con l'articolo 25 GDPR**. Inoltre **non sarebbe conforme all'articolo 5, paragrafo 1, lettera e), GDPR** sulla base delle informazioni a disposizione del Comitato e **non sarebbe conforme all'articolo 5, paragrafo 1), lettera f), e all'articolo 32 GDPR** se un titolare del trattamento si limitasse alle misure descritte in questo scenario.

Indice

Il Comitato europeo per la protezione dei dati

visti l'articolo 63 e l'articolo 64, paragrafo 2, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso: "**GDPR**"),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 10 e 22 del regolamento interno del Comitato europeo per la protezione dei dati (in appresso "**Comitato**" o "**EDPB**"),

considerando quanto segue:

(1) Il ruolo principale del Comitato è garantire l'applicazione coerente del GDPR in tutto lo Spazio economico europeo (in appresso "**SEE**"). L'articolo 64, paragrafo 2, GDPR stabilisce che qualsiasi autorità di controllo (in appresso "**AC**"), il presidente del Comitato o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro del SEE siano esaminate dal Comitato al fine di ottenere un parere.

(2) Il parere del comitato è adottato a norma dell'articolo 64, paragrafo 3, GDPR, in combinato disposto con l'articolo 10, paragrafo 2, del regolamento interno dell'EDPB, entro otto settimane dalla data in cui il presidente e l'AC competente hanno deciso che il fascicolo è completo. Su decisione del presidente, tale periodo può essere prorogato di sei settimane, tenuto conto della complessità della questione.

ha adottato il presente parere:

1 INTRODUZIONE

1.1 Sintesi dei fatti

1. Il 16 febbraio 2024 l'autorità di controllo francese (in appresso "**AC FR**") ha chiesto al Comitato di emettere un parere sulla compatibilità con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR dell'uso della tecnologia di riconoscimento facciale da parte dei gestori aeroportuali e delle compagnie aeree per l'autenticazione o l'identificazione biometrica dei passeggeri[2] al fine di snellire il flusso di questi ultimi ai punti di controllo di sicurezza aeroportuali[3], alla consegna dei bagagli, all'imbarco e all'accesso alla sala d'attesa per i passeggeri (esclusi i controlli di frontiera e i controlli

[1] Ai fini del presente parere, per "**Stati membri**" si intendono gli "Stati membri del SEE". Ai fini del presente parere, per "Unione" o "UE" si intende il "SEE".
[2] Nel contesto del presente parere, per "**passeggero**" si intende un interessato i cui dati personali sono trattati per la finalità specifica descritta nel presente parere. Nel presente parere i termini "passeggero" e "persona" sono utilizzati in modo intercambiabile.
[3] Ai fini del presente parere, per "**punti di controllo di sicurezza aeroportuali**" si intendono i controlli di sicurezza effettuati sotto la responsabilità del gestore aeroportuale cui i passeggeri devono sottoporsi per accedere dalla zona partenze all'area o alla porta di imbarco.

effettuati dai negozi sotto controllo doganale) (in appresso la "**richiesta**"). L'AC FR ha allegato alla sua richiesta una descrizione dei tipici casi d'uso (allegato I).

2. Nella sua richiesta l'AC FR osserva che i modelli attualmente in fase di sperimentazione in diversi aeroporti dell'UE variano da uno Stato membro all'altro, creando così un possibile rischio di divergenza tra le interpretazioni delle AC e il rischio che si producano effetti diversi per i diritti e le libertà fondamentali degli interessati nell'UE[4].

3. Il Comitato ritiene che, al fine di fornire una risposta alla richiesta, occorra rispondere alle domande elencate di seguito.

4. **Domanda n. 1**

1.1. L'uso della tecnologia di riconoscimento facciale per l'autenticazione biometrica **al fine specifico di snellire il flusso dei passeggeri negli aeroporti** (punti di controllo di sicurezza, consegna dei bagagli, imbarco e accesso alla sala d'attesa per i passeggeri) può essere compatibile con l'**articolo 5, paragrafo 1, lettera f)**, e con gli **articoli 25 e 32 GDPR** nel caso di un'architettura di conservazione, in cui il modello biometrico di ciascun passeggero è conservato **solo nelle mani della persona**, ad esempio localmente su un suo singolo dispositivo, sotto il suo esclusivo controllo?

1.2. Se tale trattamento fosse ritenuto compatibile con le disposizioni di cui sopra, quali garanzie minime adeguate sarebbero necessarie alla luce degli articoli 25 e 32 GDPR?

Domanda n. 2

2.1. L'uso della tecnologia di riconoscimento facciale per l'autenticazione o l'identificazione biometrica **al fine specifico di snellire il flusso dei passeggeri negli aeroporti** (punti di controllo di sicurezza, consegna dei bagagli, imbarco e accesso alla sala d'attesa per i passeggeri) può essere compatibile con l'**articolo 5, paragrafo 1, lettere e) e f)**, e con gli **articoli 25 e 32 GDPR** nel caso di un'architettura di conservazione **centralizzata**, in cui il modello biometrico di ciascun passeggero è conservato:

2.1.1. in una banca dati centrale all'interno dell'aeroporto sotto il controllo del gestore aeroportuale in forma cifrata con una chiave segreta nota esclusivamente alla persona (ad esempio nel suo telefono cellulare) ai fini dell'autenticazione?

2.1.2. Se tale trattamento fosse ritenuto compatibile, quali garanzie minime adeguate sarebbero necessarie alla luce degli articoli 25 e 32 GDPR?

2.2.1. in una banca dati centrale all'interno dell'aeroporto sotto il controllo del gestore aeroportuale in forma cifrata con chiavi in possesso di quest'ultimo ai fini dell'identificazione?

2.2.2. Se tale trattamento fosse ritenuto compatibile, quali garanzie minime adeguate sarebbero necessarie alla luce degli articoli 25 e 32 GDPR?

[4] Richiesta, pag. 1.

2.3.1. in una banca dati nel cloud sotto il controllo della compagnia aerea o del suo fornitore di servizi (responsabile del trattamento) in forma cifrata con chiavi in possesso della compagnia aerea o del suo fornitore di servizi ai fini dell'identificazione?

2.3.2. Se tale trattamento fosse ritenuto compatibile, quali garanzie minime adeguate sarebbero necessarie alla luce degli articoli 25 e 32 GDPR?

5. Dopo che l'AC FR e la presidente del Comitato hanno ritenuto il fascicolo completo rispettivamente il 16 e il 23 febbraio 2024, il fascicolo è stato distribuito dal segretariato il 23 febbraio 2024. La presidente del Comitato ha deciso, in conformità dell'articolo 64, paragrafo 3, GDPR, in combinato disposto con l'articolo 10, paragrafo 2, del regolamento interno dell'EDPB, di prorogare di ulteriori sei settimane il termine (normalmente pari a otto settimane), tenuto conto della complessità della questione.

1.2 Ammissibilità della richiesta di un parere relativo all'articolo 64, paragrafo 2, GDPR

6. L'articolo 64, paragrafo 2, GDPR stabilisce che in particolare qualsiasi AC può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal Comitato al fine di ottenere un parere.

7. Il Comitato ritiene che la richiesta presentata dall'AC FR sulla compatibilità dell'uso della tecnologia di riconoscimento facciale per l'autenticazione o l'identificazione biometrica al fine specifico di snellire il flusso dei passeggeri negli aeroporti riguardi questioni "che producono effetti in più di uno Stato membro", in quanto, come spiegato nella richiesta[5], esistono attualmente diversi progetti in fase di realizzazione negli aeroporti degli Stati membri e si prevede che tale uso aumenterà nei prossimi anni. I modelli al momento in fase di sperimentazione da parte di diversi aeroporti e compagnie aeree variano notevolmente da uno Stato membro all'altro, creando così il possibile rischio che, dal punto di vista della protezione dei dati, si producano effetti divergenti in più di uno Stato membro.

8. Inoltre il Comitato ritiene che la richiesta presentata dall'AC FR abbia conseguenze importanti per l'applicazione dei principi di cui all'articolo 5, paragrafo 1, lettere e) e f), GDPR, e dei requisiti applicabili ai titolari del trattamento di cui all'articolo 25 GDPR, nonché dei requisiti applicabili ai titolari del trattamento e ai responsabili del trattamento di cui all'articolo 32 GDPR. Pertanto la presente richiesta riguarda una "questione di applicazione generale" ai sensi dell'articolo 64, paragrafo 2, GDPR, in quanto si riferisce all'interpretazione coerente dei principi di limitazione della conservazione (articolo 5, paragrafo 1, lettera e), GDPR) e di integrità e riservatezza (articolo 5, paragrafo 1, lettera f), GDPR), nonché delle nozioni di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (articolo 25 GDPR) e di sicurezza dei dati (articolo 32 GDPR), al fine di garantire tra l'altro l'applicazione coerente di tali disposizioni nel SEE.

9. Eventuali posizioni divergenti tra gli Stati membri sull'interpretazione dell'articolo 5, paragrafo 1, lettere e) e f), e degli articoli 25 e 32 GDPR amplificherebbero il rischio che i gestori aeroportuali e le compagnie aeree sviluppino progetti di riconoscimento facciale in modo non coerente. Dal momento che l'AC FR ha dimostrato la chiara necessità di un'interpretazione coerente di tali disposizioni in relazione alla tecnologia di riconoscimento facciale per l'autenticazione o l'identificazione biometrica

[5] Richiesta, pag. 3.

dei passeggeri al fine di snellire il flusso dei passeggeri negli aeroporti[6], il Comitato ritiene che la richiesta sia motivata in linea con l'articolo 10, paragrafo 3, del regolamento interno dell'EDPB.

10. Ai sensi dell'articolo 64, paragrafo 3, GDPR, l'EDPB non emette un parere qualora abbia già formulato un parere sulla questione[7]. L'EDPB non ha ancora fornito risposte alle domande derivanti dalla richiesta. Sebbene forniscano già alcuni elementi utili sulle misure di sicurezza che dovrebbero essere applicate al trattamento dei dati biometrici, le linee guida 3/2019 dell'EDPB sui dispositivi video[8] non affrontano tutti gli aspetti relativi alle domande sollevate nella richiesta. Inoltre le linee guida dell'EDPB disponibili, comprese le linee guida 3/2019 dell'EDPB sui dispositivi video, non forniscono indicazioni specifiche sui possibili elementi da verificare in relazione alla conservazione centralizzata o decentralizzata dei dati biometrici per identificare o autenticare i passeggeri al fine di snellire il flusso di questi ultimi negli aeroporti e sulla compatibilità di tale trattamento con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR.

11. Per questi motivi il Comitato ritiene che la richiesta sia ricevibile e che le domande sollevate dovrebbero essere esaminate in un parere adottato a norma dell'articolo 64, paragrafo 2, GDPR.

2 AMBITO DI APPLICAZIONE E CONTESTO DEL PARERE

2.1 Ambito di applicazione del parere

12. Il presente parere riguarda solo la compatibilità con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GPDR dell'uso della tecnologia di riconoscimento facciale per l'autenticazione o l'identificazione biometrica dei passeggeri da parte dei gestori aeroportuali e delle compagnie aeree **al fine specifico di snellire il flusso dei passeggeri negli aeroporti**, ossia ai punti di controllo di sicurezza, alla consegna dei bagagli, all'imbarco e all'accesso alla sala d'attesa per i passeggeri, come indicato nella richiesta.

13. Per quanto riguarda **l'ambito di applicazione del presente parere**, il Comitato chiarisce quanto segue:

    1) il trattamento dei dati personali nell'ambito dei controlli di frontiera e dei controlli effettuati dai negozi sotto controllo doganale non rientra nell'ambito di applicazione del presente parere, in quanto effettuato da titolari del trattamento diversi dai gestori aeroportuali e dalle compagnie aeree;

    2) l'uso della tecnologia di riconoscimento facciale, anche se basato sugli scenari descritti di seguito nella sezione 3.2, per qualsiasi altra finalità (come l'attività di contrasto) o da parte di qualsiasi altra persona, anche se per finalità analoghe, esula dall'ambito di applicazione del presente parere;

    3) il presente parere esamina solo il trattamento dei dati personali dei passeggeri e non riguarda altri tipi di interessati, come il personale dei gestori aeroportuali o delle compagnie aeree;

[6] Richiesta, pagg. 1-3.
[7] Articolo 64, paragrafo 3, GDPR e articolo 10, paragrafo 4, del regolamento interno dell'EDPB.
[8] EDPB, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, versione 2.0, adottate il 29 gennaio 2020 (in appresso "**linee guida 3/2019 dell'EDPB sui dispositivi video**").

4) il presente parere esamina la richiesta presentata dall'AC FR in relazione alla compatibilità delle architetture di conservazione dei modelli biometrici dei passeggeri con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR. A tale riguardo il presente parere non include un'analisi completa ed esaustiva della conformità al GDPR da parte del relativo titolare o dei relativi titolari del trattamento in ciascun caso, nonché del loro responsabile o dei loro responsabili del trattamento, se del caso. Ciò è particolarmente importante se si considera che tali tecnologie comportano maggiori rischi associati al trattamento di categorie particolari di dati a norma dell'articolo 9 GDPR. Il presente parere non pregiudica pertanto una valutazione relativa ad altre disposizioni del GDPR per quanto riguarda l'uso di tecnologie di riconoscimento facciale, anche nel settore specifico oggetto della richiesta o un'analisi giuridica e tecnica caso per caso basata sulle circostanze e sul trattamento specifici previsti da un titolare del trattamento;

5) il presente parere non esamina il trattamento dei dati personali dei minori e non pregiudica gli eventuali requisiti specifici applicabili a tale riguardo;

6) il presente parere non pregiudica i requisiti di legge e le ulteriori limitazioni all'uso dei dati biometrici derivanti dal diritto nazionale degli Stati membri[9];

7) qualsiasi conclusione contenuta nel presente parere non pregiudica gli ulteriori sviluppi tecnologici;

8) il presente parere prende in esame quattro scenari, le cui caratteristiche specifiche sono descritte di seguito nella sezione 3.2, e non si occupa di altri scenari, anche se il trattamento è effettuato per le stesse finalità.

14. Nella sua richiesta l'AC FR ha indicato che il trattamento dei dati biometrici dei passeggeri al fine di snellire il flusso di questi ultimi negli aeroporti si baserebbe sul presupposto che le persone acconsentano a tale trattamento, il che costituirebbe eventualmente la base giuridica ai sensi del GDPR[10]. **Tuttavia l'analisi della base giuridica applicabile non rientra nell'ambito delle domande sottoposte all'EDPB nella richiesta e pertanto la validità del consenso per tale trattamento ai sensi degli articoli 6, 7 e 9 GDPR non è esaminata nel presente parere.**

15. Ciononostante l'EDPB osserva in termini generali che, se dovessero fare affidamento su tale base giuridica, i relativi titolari del trattamento sarebbero tenuti a ottenere un valido consenso esplicito[11] da parte delle persone disposte a utilizzare tali servizi. Detto consenso esplicito dovrebbe essere

[9] Ad esempio l'articolo 9, paragrafo 4, GDPR prevede che gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati biometrici.
[10] Richiesta, allegato I.
[11] A norma dell'articolo 4, punto 14, e dell'articolo 9, paragrafo 1, nonché dell'articolo 9, paragrafo 2, lettera a), GDPR, il trattamento dei dati biometrici intesi a identificare in modo univoco una persona fisica è vietato, a meno che l'interessato non abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui all'articolo 9, paragrafo 1, GDPR. Cfr. anche i considerando 51, 52, e 53 GDPR.

liberamente prestato, specifico e informato[12] e il soddisfacimento di tali condizioni sarebbe esaminato caso per caso. Ciò significa tra l'altro che:

1) le persone dovrebbero poter revocare facilmente tale consenso in qualsiasi momento e senza subire pregiudizio[13];

2) affinché il consenso sia liberamente prestato, tale uso delle tecnologie biometriche può avvenire solo su base volontaria, in quanto le persone dovrebbero poter scegliere liberamente se utilizzare o meno tali servizi e senza subire pregiudizio (ad esempio ritardi significativamente più lunghi per i passeggeri che non prestano il proprio consenso[14]), incentivi, costi aggiuntivi o vantaggi aggiuntivi in cambio[15];

3) il consenso esplicito dovrebbe essere richiesto anche alle persone i cui dati biometrici sono oggetto di trattamento, anche se non si sono registrati ai fini dell'identificazione o dell'autenticazione con tali mezzi. In altre parole è essenziale che il volto delle persone che non hanno esplicitamente acconsentito al riconoscimento facciale per la finalità prevista non sia scansionato dalle videocamere. Ciò può essere conseguito ad esempio dedicando corsie specifiche al riconoscimento facciale e garantendo una segnaletica adeguata e una separazione fisica con i flussi di controllo non biometrici per consentire una chiara identificazione di tali corsie;

4) fatta salva l'eventualità che il consenso sia la base giuridica applicabile per tale trattamento, i principi applicabili al trattamento sanciti dall'articolo 5 GDPR per quanto concerne la necessità e la proporzionalità continuano ad applicarsi anche quando le persone hanno prestato il proprio consenso esplicito all'uso dei loro dati biometrici[16].

16. La richiesta specifica[17] che i gestori aeroportuali agiranno in qualità di titolari del trattamento per quanto riguarda il trattamento presso i punti di controllo di sicurezza aeroportuali, mentre le compagnie aeree agiranno in qualità di titolari del trattamento per quanto riguarda la consegna dei bagagli, l'imbarco e l'accesso alla sala d'attesa per i passeggeri. Pertanto il Comitato osserva che diversi attori potrebbero essere coinvolti nel trattamento descritto nella richiesta e non ha valutato l'applicazione dei ruoli di (con)titolare del trattamento e/o responsabile del trattamento negli scenari descritti di seguito nella sezione 3.2 del presente parere. In ogni caso occorre individuare gli attori coinvolti e ripartire chiaramente le loro responsabilità, in modo da soddisfare i requisiti del GDPR[18].

---

[12] Articolo 4, punto 11, e articolo 7 GDPR.
[13] Articolo 7, paragrafo 4, e considerando 50 GDPR.
[14] Ad esempio ciò potrebbe includere considerazioni quali la progettazione di un sistema per evitare di creare una pressione sociale sui passeggeri che non desiderano prestare il proprio consenso, evitando che la loro scelta abbia un impatto negativo sugli altri passeggeri.
[15] EDPB, *Linee guida 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, versione 1.1, adottate il 4 maggio 2020 (in appresso "**linee guida 05/2020 dell'EDPB sul consenso**"), punti 46 e 48.
[16] Ibidem, punto 5.
[17] Richiesta, allegato I.
[18] In linea con l'articolo 4, punti 7 e 8, l'articolo 5, paragrafo 2, e gli articoli 24, 26, 28 e 29 GDPR. Cfr. anche EDPB, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, versione 2.1, adottate il 7 luglio 2021.

17. Inoltre il Comitato osserva che attualmente nell'UE non esiste alcun requisito di legge uniforme che impone ai gestori aeroportuali e alle compagnie aeree di identificare i passeggeri e verificare che il nome sulla loro carta d'imbarco corrisponda a quello riportato sul loro documento d'identità in tutti i suddetti punti di controllo[19]. Pertanto tali requisiti sono soggetti alle norme del diritto nazionale che possono variare da uno Stato membro all'altro. In alcuni Stati membri tale verifica può essere richiesta per alcuni punti di controllo (ad esempio la consegna dei bagagli o l'imbarco), mentre in altri non sono attualmente necessari controlli di questo tipo[20]. L'esistenza di obblighi giuridici intesi a verificare l'identità dei passeggeri ha un impatto diretto sulle prassi adottate dai diversi aeroporti.

18. Di conseguenza, in tali situazioni, **in cui non è richiesta alcuna verifica dell'identità dei passeggeri mediante un documento d'identità ufficiale, non dovrebbe essere effettuata alcuna verifica con l'uso di dati biometrici, in quanto determinerebbe un trattamento eccessivo dei dati, dal momento che comporta il trattamento di dati aggiuntivi rispetto alla situazione attuale e non si limiterebbe a quanto necessario per la finalità pertinente, in violazione del principio di minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), GDPR**. Tale considerazione dovrebbe essere tenuta presente in relazione all'esame di tutti gli scenari descritti di seguito nella sezione 3.2 del presente parere.

2.2 Concetti di base

19. Per qualificarsi come dati biometrici ai sensi dell'articolo 4, punto 14, GDPR[21], il trattamento di dati grezzi, come le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, dovrebbe comprendere una misurazione di tali caratteristiche, poiché i dati biometrici sono il risultato di tali misurazioni[22].

20. Prendendo l'immagine di un volto di una persona (una fotografia o un video) detto "**campione**" biometrico, è possibile estrarre una rappresentazione digitale (che è detta "**modello**") delle caratteristiche distinte di tale volto[23]. Inoltre il Comitato ricorda che "[u]n modello biometrico è una rappresentazione digitale delle caratteristiche uniche estratte da un campione biometrico che possono essere memorizzate in una banca dati biometrica"[24] che consente o conferma l'identificazione univoca di una persona fisica. Inoltre "[q]uesto modello [biometrico] dovrebbe essere

[19] La normativa pertinente a livello di UE è il regolamento di esecuzione (UE) 2015/1998 della Commissione, del 5 novembre 2015, che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea. Tuttavia tale regolamento non riguarda i controlli dei documenti d'identità ufficiali ai punti di controllo negli aeroporti e gli Stati membri hanno la facoltà di disciplinare tale aspetto a livello nazionale.

[20] Ciò significa che attualmente non è effettuata alcuna verifica o è verificata solo l'esistenza della carta d'imbarco. Ad esempio, sulla base del protocollo del 22 maggio 1954 relativo all'esenzione dei cittadini di Danimarca, Finlandia, Norvegia e Svezia dall'obbligo di possedere un passaporto o un permesso di soggiorno durante il periodo di soggiorno in un paese scandinavo diverso dal proprio, a decorrere dal 1º luglio 1954 i cittadini di Danimarca, Finlandia, Norvegia e Svezia sono esentati dall'obbligo di essere in possesso di un passaporto o di un altro documento d'identità quando viaggiano tra questi paesi.

[21] Cfr. anche i considerando 51, 52 e 53 GDPR.

[22] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 74.

[23] EDPB, *Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto*, versione 2.0, adottate il 26 aprile 2023 (in appresso "**linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto**"), punti 7 e 8.

[24] Ibidem, punto 9.

unico e specifico per ogni persona e, in linea di principio, è immutabile nel tempo"[25]. Di norma in un processo di confronto finalizzato all'identificazione o all'autenticazione di una persona tramite il riconoscimento facciale un modello biometrico in entrata è confrontato con gli oggetti conservati per verificare una corrispondenza o trovarne una in una banca dati[26].

21. La tecnologia di riconoscimento facciale può svolgere due funzioni distinte: autenticazione[27] e identificazione[28]. Benché ambedue le funzioni siano distinte, entrambe si basano sul trattamento di dati biometrici relativi a una persona fisica identificata o identificabile[29] e costituiscono dunque un trattamento di categorie particolari di dati personali ai sensi dell'articolo 9 GDPR[30].

22. In particolare:

    l'**autenticazione** mira a confermare le caratteristiche biometriche rivendicate mediante il confronto ed è anche detta verifica 1:1;

    l'**identificazione** mira a ricercare in una banca dati di registrazione biometrica identificativi attribuibili a una singola persona ed è detta anche identificazione 1:molti.

23. In entrambi i casi (identificazione e autenticazione) le tecniche di riconoscimento facciale si basano su una corrispondenza stimata tra modelli: ossia quello confrontato e quello/i di riferimento. Da questo punto di vista, si tratta di tecniche probabilistiche: dal confronto emerge una probabilità maggiore o minore che la persona sia effettivamente quella da autenticare o identificare; se questa probabilità supera un determinato valore soglia nel sistema, definito dal suo sviluppatore o dall'utente, il sistema presupporrà che vi sia una corrispondenza da autenticare o identificare[31].

[25] Ibidem.
[26] Linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto, punti 10 e 11; cfr. anche la norma internazionale ISO/IEC 2382-37, 2022-03,
disponibile all'indirizzo: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073514_ISO_IEC%202382-37_2022(E).zip [ultima consultazione 23 maggio 2024] (in appresso "**ISO/IEC 2382-37**").
[27] Il Comitato osserva che l'imminente regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) (non ancora pubblicato nella *Gazzetta ufficiale*) definisce anche, all'articolo 3, punto 36, la "verifica biometrica" come "la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza" (cfr. la risoluzione legislativa del Parlamento europeo del 13 marzo 2024 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (COM(2021) 0206 – C9-0146/2021 – 2021/0106(COD)).
[28] Ibidem, l'articolo 3, paragrafo 35, della legge sull'intelligenza artificiale definisce l'"identificazione biometrica" come "il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati".
[29] ISO/IEC 2382-37.
[30] Articolo 4, punto 14, GDPR e linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto, punto 12.
[31] Linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto, punto 11. Cfr. anche ISO/IEC 2382-37.

3 SUL MERITO DELLA RICHIESTA

3.1 Osservazioni generali

24. La presente sezione esamina le domande sollevate al punto 4. In tale contesto il Comitato esaminerà, per la domanda 1, la compatibilità con l'articolo 5, paragrafo 1, lettera f), e con gli articoli 25 e 32 GDPR e, per la domanda 2, la compatibilità con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR.

25. A tal fine il Comitato esaminerà quattro diversi scenari[32], le cui caratteristiche specifiche sono descritte nella sezione 3.2.

26. Come osservazione preliminare, il Comitato ricorda che l'uso dei dati biometrici e in particolare della tecnologia di riconoscimento facciale comporta maggiori rischi per i diritti e le libertà degli interessati. In primo luogo il trattamento in questione riguarda i dati biometrici cui è accordata una protezione particolare ai sensi dell'articolo 9 GDPR. In particolare i dati biometrici cambiano in maniera irreversibile la relazione tra corpo e identità, in quanto le caratteristiche del corpo umano possono essere "lette" da una macchina e sottoposte a un successivo trattamento[33]. Inoltre l'uso della tecnologia di riconoscimento facciale può comportare rischi associati a falsi negativi, distorsioni e discriminazioni[34] e il rischio di un uso improprio dei dati biometrici potrebbe avere gravi conseguenze per le persone, come l'usurpazione d'identità o l'impersonificazione[35]. È inoltre opportuno osservare che, quando il riconoscimento facciale è effettuato a distanza e senza il coinvolgimento attivo dell'interessato, le persone potrebbero essere ancora meno consapevoli di tale trattamento e dei rischi associati. Infine è importante sottolineare che le caratteristiche su cui si basano i dati biometrici possono generalmente essere considerate permanenti e dovrebbero essere trattate in modo irreversibile, in particolare nel contesto del riconoscimento facciale[36].

27. Pertanto, alla luce di quanto precede, prima di utilizzare tali tecnologie, anche se dovessero essere ritenute particolarmente efficaci, i titolari del trattamento dovrebbero valutare l'impatto sui diritti e sulle libertà fondamentali degli interessati e considerare se mezzi meno invasivi possano raggiungere la finalità legittima del rispettivo trattamento[37].

---

[32] I quattro scenari esaminati dal Comitato si basano sui casi d'uso presentati nell'allegato I della richiesta. L'AC FR ha chiarito che i casi d'uso presentati nell'allegato I della richiesta sono esempi di attuazione, appartenenti a uno scenario, utilizzati a fini illustrativi.

[33] Gruppo di lavoro articolo 29, *Parere 3/2012 sugli sviluppi nelle tecnologie biometriche*, adottato il 27 aprile 2012, WP193 (in appresso "**parere 3/2012 del Gruppo di lavoro articolo 29 sulle tecnologie biometriche**"), pag. 4. È opportuno osservare che il presente parere fa riferimento alla direttiva 95/46/CE, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("direttiva sulla protezione dei dati"). Il GDPR ha ampliato l'ambito di applicazione delle categorie particolari di dati e, a differenza della direttiva sulla protezione dei dati, prevede che i dati biometrici rientrino tra le categorie particolari di dati (articolo 9 GDPR).

[34] *Guidelines on facial recognition, Consultative Committee of Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data*, giugno 2021, pag. 15; anche le linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto, punto 27.

[35] Parere 3/2012 del Gruppo di lavoro articolo 29 sulle tecnologie biometriche, pag. 29.

[36] Linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto, punto 104.

[37] Considerando 39 GDPR. Cfr. anche le linee guida 3/2019 dell'EDPB sui dispositivi video, punto 73.

28. Il Comitato ricorda inoltre che il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta e dovrebbe essere contemperato con altri diritti fondamentali tutelati dalla Carta, in ossequio al principio di proporzionalità[38].

29. L'articolo 25, paragrafo 1, GDPR fa riferimento ai "principi di protezione dei dati" elencati all'articolo 5 GDPR[39] e impone di attuarli fin dalla progettazione "in modo efficace"[40]. Ciò include espressamente il principio della minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), GDPR[41], secondo cui i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati e che dà espressione al suddetto principio di proporzionalità"[42]. Inoltre l'articolo 25, paragrafo 2, GDPR indica l'obbligo di "minimizzazione dei dati per impostazione predefinita", affermando che tale obbligo vale per la quantità di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità dei dati[43].

30. Tuttavia l'articolo 25 GDPR non richiede ai titolari del trattamento l'attuazione di misure tecniche e organizzative specifiche, bensì che le misure e le garanzie scelte siano specificamente connesse al contesto e ai rischi per i diritti e le libertà dell'interessato posti dal trattamento[44]. Analogamente l'articolo 32 GDPR sulla sicurezza del trattamento impone ai titolari del trattamento e ai responsabili del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche.

31. È importante sottolineare che, anche se i passeggeri dovessero acconsentire esplicitamente all'uso dei loro dati biometrici al fine di snellire il flusso di passeggeri negli aeroporti, i principi applicabili al

---

[38] Considerando 4 GDPR. Cfr. anche a questo proposito la sentenza della Corte di giustizia del 22 giugno 2021, *Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504 (in appresso "C-439/19 *Latvijas Republikas Saeima*"), punti 98, 110 e 113. Inoltre il principio di proporzionalità, in quanto principio generale del diritto dell'Unione, esige che gli strumenti istituiti da un atto dell'Unione siano idonei a realizzare l'obiettivo perseguito e non vadano oltre quanto è necessario per raggiungerlo (cfr. sentenza della Corte di giustizia del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, C-92/09 e C-93/09, ECLI:EU:C:2010:662 (in appresso "C-92/09 e C-93/09 *Volker und Schecke*"), punto 74 e giurisprudenza ivi citata).

[39] EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, versione 2.0, adottate il 20 ottobre 2020 (in appresso "**linee guida 4/2019 dell'EDPB sulla protezione dei dati fin dalla progettazione e per impostazione predefinita**"), punto 11.

[40] L'articolo 25, paragrafo 1, GDPR stabilisce che: "[t]enendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati". Cfr. anche EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, punto 13.

[41] Analogamente il considerando 39 GDPR stabilisce che i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.

[42] C-439/19 *Latvijas Republikas Saeima*, punto 98; sentenza della Corte di giustizia dell'11 dicembre 2019, *Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064 (in appresso "C-708/18 *M5A-ScaraA*"), punto 48.

[43] EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, punto 48.

[44] EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, punto 14.

trattamento sanciti dal GDPR per quanto concerne la necessità e la proporzionalità continuano ad applicarsi e devono essere rispettati[45].

32. Per quanto riguarda il **principio di necessità**, il Comitato valuterà se il trattamento proposto sia necessario per conseguire l'obiettivo perseguito e se lo stesso obiettivo possa essere raggiunto in modo altrettanto efficace mediante altri mezzi meno invasivi dei diritti e delle libertà fondamentali dell'interessato[46]. Per quanto riguarda il **principio di proporzionalità**, il Comitato valuterà se l'impatto negativo sui diritti e sulle libertà fondamentali degli interessati sia proporzionato a eventuali vantaggi previsti. Se il vantaggio è relativamente modesto, tale impatto potrebbe non essere proporzionato[47].

33. In ogni caso, anche se il Comitato ritiene che uno degli scenari esaminati di seguito potrebbe soddisfare i requisiti di cui all'articolo 5, paragrafo 1, lettere e) e f), e agli articoli 25 e 32 GDPR, spetta in ogni caso al titolare del trattamento dimostrarlo con elementi di fatto. Tale dimostrazione dovrebbe includere l'esame di scenari alternativi.

3.2 Sulla compatibilità con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR

3.2.1 Scenario 1: conservazione del modello biometrico registrato solo nelle mani della persona ai fini dell'autenticazione

34. La presente sezione esamina la compatibilità con l'articolo 5, paragrafo 1, lettera f), e con gli articoli 25 e 32 GDPR della conservazione del modello biometrico dei passeggeri solo nelle mani della persona, ad esempio su un suo singolo dispositivo[48], sotto il suo esclusivo controllo[49], ai fini dell'autenticazione[50] (in appresso "**scenario 1**"). La presente sezione esamina anche le garanzie adeguate per lo scenario 1 alla luce degli articoli 25 e 32 GDPR.

Descrizione dello scenario

35. Nello scenario 1 il modello biometrico registrato di ciascun passeggero, che ha acconsentito a tale trattamento, è conservato solo nelle mani della persona, ad esempio su un singolo dispositivo di ogni passeggero, sotto il suo esclusivo controllo. I passeggeri sono autenticati (confronto 1:1) quando attraversano specifici punti di controllo in aeroporto.

36. La registrazione è effettuata dal gestore aeroportuale a distanza tramite l'applicazione di quest'ultimo[51] o presso i terminal aeroportuali a un livello di garanzia dell'identità adeguato (ad

[45] Linee guida 5/2020 dell'EDBP sul consenso ai sensi del regolamento (UE) 2016/679, punto 5.
[46] C-439/19 *Latvijas Republikas Saeima*, punti 110 e 113; Sentenza della Corte di giustizia (Grande Sezione) del 4 luglio 2023, *Meta v. Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537, punto 108.
[47] C-708/18 *M5A-ScaraA*, punti da 52 a 56, C-92/09 e C-93/09 *Volker und Schecke*, punto 87; C-439/19 *Latvijas Republikas Saeima*, punti 98, 110 e 113. Cfr. anche il parere 3/2012 del Gruppo di lavoro articolo 29 sulle tecnologie biometriche, pag. 8.
[48] In alternativa la persona potrebbe stampare e conservare il proprio modello biometrico su carta.
[49] Ciò non pregiudica la responsabilità generale del titolare del trattamento per quanto riguarda il trattamento.
[50] Come esemplificato dal caso d'uso 1 nell'allegato I della richiesta.
[51] L'EDPB osserva che in futuro potrebbero essere previste modalità alternative per tale registrazione e che la registrazione potrebbe essere effettuata senza un'applicazione specifica di un gestore aeroportuale, ad esempio attraverso l'interazione con il portafoglio digitale di un utente.

esempio eIDAS[52]). Tale registrazione consiste nella registrazione di un modello biometrico e dei dati di identificazione[53] necessari per il trattamento sul dispositivo del passeggero. La registrazione avviene una sola volta e per un periodo di validità specifico (ad esempio in linea con il periodo di validità del passaporto dei passeggeri). Né i dati di identificazione dei passeggeri, né i loro dati biometrici sono conservati dal gestore aeroportuale dopo il processo di registrazione.

37. In particolare, per quanto riguarda la conservazione, i dati di identificazione e il modello biometrico del passeggero sono conservati localmente sul dispositivo di ciascuna persona (ad esempio nell'applicazione mobile del gestore aeroportuale o in un'applicazione del portafoglio digitale). Il dispositivo può quindi essere utilizzato per trasmettere o interrogare i dati di identificazione e il modello biometrico dei passeggeri, eventualmente includendo le informazioni di volo e/o la carta d'imbarco. Ad esempio tali informazioni sono cifrate con una chiave in possesso esclusivamente del gestore aeroportuale, eventualmente codificata sotto forma di codice QR, che può essere stampato su carta o visualizzato sullo schermo del dispositivo del passeggero. In questo caso il passeggero mostrerebbe tale codice QR in apposite postazioni di controllo in aeroporto dotate di uno scanner QR e di una videocamera.

38. In termini di sicurezza, durante il confronto, i codici QR sono decifrati con una chiave in possesso del gestore aeroportuale, che è l'unico in grado di decifrare i codici QR. I dati biometrici dei passeggeri sono conservati solo per un periodo molto breve e cancellati una volta completato il confronto. È opportuno osservare che le misure di sicurezza, per quanto riguarda la conservazione, dipendono in parte dalla sicurezza del dispositivo del passeggero.

Valutazione dell'EDPB

39. Lo scenario 1 descrive le misure tecniche e organizzative intese a garantire un livello di sicurezza adeguato ai rischi per gli interessati, come richiesto dall'articolo 5, paragrafo 1, lettera f), e dall'articolo 32 GDPR. I passeggeri sono autenticati (confronto 1:1) quando attraversano specifici punti di controllo in aeroporto. In questo scenario la principale operazione di confronto è effettuata nel contesto di un ambiente controllato[54], in cui i passeggeri sono attivamente coinvolti e hanno un maggiore controllo sui loro dati. In particolare, sarebbero controllati solo i passeggeri che hanno acconsentito a tale trattamento e, dal momento che sarebbero stati controllati in postazioni dedicate, non sarebbero raccolti i dati biometrici di altri passeggeri che non vi hanno acconsentito. Inoltre i passeggeri consenzienti hanno la possibilità di interrompere il trattamento in qualsiasi momento cancellando i dati dal loro dispositivo.

[52] Un quadro in materia di identificazione elettronica e servizi fiduciari (in appresso "**eIDAS**") basato sul regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

[53] Ai fini del presente parere, per dati di identificazione si intendono dati quali cognome, nome, data di nascita ecc. la cui esattezza è stata verificata in relazione a un documento d'identità o un passaporto.

[54] Per "ambiente non controllato" si intende l'uso del riconoscimento facciale a fini di identificazione senza il coinvolgimento attivo degli interessati, in cui il modello di ogni volto che entra nell'area di monitoraggio viene confrontato con i modelli di un'ampia sezione trasversale della popolazione, conservati in una banca dati, cfr. le linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto, punto 17.

40. L'uso del riconoscimento facciale basato su un modello biometrico conservato solo nelle mani della persona, che può ad esempio essere su un singolo dispositivo del passeggero, sotto il suo esclusivo controllo, utilizzato a fini di autenticazione in specifici punti di controllo attraverso un'interfaccia dedicata, comporta, a determinate condizioni, minori rischi rispetto all'uso dei dati biometrici quando i dati sono conservati in una banca dati centralizzata[55]. Tale conservazione localizzata, se accompagnata da garanzie adeguate[56], riduce la gravità delle violazioni dei dati personali rispetto alla conservazione centralizzata in termini di numero di persone interessate e garantisce che l'accesso al modello biometrico comporti un coinvolgimento attivo dell'interessato.

41. Inoltre il confronto potrebbe essere effettuato a livello locale in aeroporto, confrontando il modello biometrico, ad esempio contenuto nel codice QR, con l'output del modello calcolato sulla base del campione biometrico rilevato dalla telecamera nella postazione di controllo. Solo il risultato del confronto sarebbe reso noto al titolare del trattamento che effettua un controllo specifico (che potrebbe essere un gestore aeroportuale o una compagnia aerea a seconda che tale controllo sia effettuato ai punti di controllo di sicurezza aeroportuali, alla consegna dei bagagli, all'imbarco e/o all'accesso alla sala d'attesa per i passeggeri) e utilizzato dallo stesso. Inoltre il fatto che le informazioni richieste per il confronto (ad esempio il codice QR) debbano essere fornite dalla persona funge da secondo fattore[57] e rafforza quindi la sicurezza dell'autenticazione.

42. Per quanto riguarda la compatibilità con l'articolo 25 GDPR e in particolare al fine di conformarsi al requisito della minimizzazione dei dati, è opportuno garantire che il trattamento soddisfi il principio di necessità. Nello scenario 1 si potrebbe ritenere che le misure scelte abbiano soddisfatto il principio di necessità in relazione alla finalità perseguita (ossia snellire il flusso dei passeggeri) se, a seconda delle circostanze del trattamento, il titolare del trattamento può dimostrare che non esistono soluzioni alternative meno invasive in grado di conseguire lo stesso obiettivo in modo altrettanto efficace. Ad esempio il titolare del trattamento può essere in grado di dimostrare che, anche se i passeggeri dovessero mostrare il loro dispositivo, lo scenario 1 accelera il processo di verifica rispetto alla situazione attuale, che prevede la verifica umana della corrispondenza tra il nome sulla carta d'imbarco e il documento d'identità del passeggero[58]. In particolare ciò non potrebbe essere dimostrato se attualmente non si effettuano controlli per verificare l'identità dei passeggeri sulla base del loro documento d'identità ufficiale (a tale riguardo cfr. punto 18).

43. Inoltre i modelli biometrici non sono conservati dal gestore aeroportuale dopo la registrazione e il periodo di conservazione dei dati biometrici da parte del titolare del trattamento che effettua il controllo è molto breve, in quanto tali dati sono cancellati non appena il confronto è stato completato. Pertanto le misure scelte nello scenario 1 sembrano limitare la portata del trattamento e il periodo di conservazione dei dati personali.

44. Per quanto riguarda il principio di proporzionalità, l'invasività derivante da tale trattamento può essere controbilanciata dal coinvolgimento attivo dei passeggeri, in quanto i dati biometrici di questi ultimi sarebbero conservati solo nelle loro mani. Inoltre, tenendo conto delle misure sopra descritte

[55] Linee guida 05/2022 dell'EDPB sul riconoscimento facciale nelle attività di contrasto, punto 17.
[56] Come illustrato dal punto 46.
[57] Ciò attenua ad esempio il rischio di *spoofing* dell'identità. Cfr. anche la garanzia C.1.2.
[58] Si potrebbe inoltre sostenere che il controllo biometrico può essere meno soggetto ad errori rispetto al controllo umano.

e supponendo che il titolare del trattamento attui garanzie adeguate come richiesto dallo specifico trattamento in questione, l'attuazione di misure adeguate potrebbe garantire un livello di sicurezza adeguato al rischio. In tal caso l'impatto negativo sui diritti e sulle libertà fondamentali degli interessati potrebbe essere considerato proporzionato al vantaggio previsto.

45. Pertanto, tenendo conto di quanto precede, in risposta alla domanda 1.1, il Comitato conclude che tale trattamento **potrebbe essere considerato in linea di principio compatibile con l'articolo 5, paragrafo 1, lettera f), e con gli articoli 25 e 32 GDPR, fatte salve le garanzie adeguate**.

Garanzie adeguate

46. In questo tipo di scenario, in risposta alla domanda 1.2, l'EDPB ritiene che debbano essere attuate almeno le garanzie seguenti. Garanzie diverse da quelle descritte nel presente parere potrebbero essere utilizzate per conseguire gli stessi obiettivi di sicurezza e protezione dei dati e potrebbero essere lecite purché garantiscano la conformità al quadro giuridico applicabile.

47. Nota: si tratta di una panoramica di alto livello e non esaustiva delle possibili garanzie adeguate, che dovrebbero essere attuate da un titolare del trattamento in una soluzione simile allo scenario 1. La loro adeguatezza ai sensi degli articoli 25 e 32 GDPR dipenderà da un'analisi caso per caso. Tutti i titolari del trattamento dovranno assicurarsi di effettuare la propria valutazione d'impatto sulla protezione dei dati (in appresso "DPIA")[59] e le loro soluzioni specifiche possono richiedere misure supplementari non incluse nel presente parere.

A. Considerazioni generali

A.1 Valutazione d'impatto sulla protezione dei dati

A.1.1 Effettuare una DPIA, in linea con i requisiti dell'articolo 35 GDPR, ogniqualvolta il titolare del trattamento preveda un nuovo trattamento che comporti a sua volta un trattamento che può presentare un rischio elevato. Questo è probabilmente il caso dello scenario 1, in quanto comporta il trattamento di dati biometrici su larga scala[60]. Valutare l'opportunità di attuare un sistema di riconoscimento facciale, compresa la sua necessità e proporzionalità in relazione alle finalità perseguite[61], durante la fase iniziale di progettazione e riesaminarlo durante l'intero ciclo di vita dello sviluppo del prodotto.

A.1.2 Consultare l'autorità di controllo competente qualora il trattamento presenti ancora un rischio elevato nonostante le misure adottate dal titolare del trattamento per attenuare il rischio[62].

[59] Articolo 35 GDPR.
[60] Articolo 35, paragrafo 3, GDPR e Gruppo di lavoro Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, WP 248 rev.01, approvate dall'EDPB.
[61] Articolo 35, paragrafo 7, lettera b), GDPR.
[62] Articolo 36, paragrafo 1, GDPR.

A.2 Diritti degli interessati e garanzie che possono essere attuate dai titolari del trattamento

A.2.1 Garanzie per affrontare i casi di falsi negativi. Attenuare il rischio di distorsioni legate all'età, al genere e alla razza "valuta[ndo] periodicamente se gli algoritmi funzionino in linea con le finalità e adegua[ndoli] per attenuare le distorsioni individuate e garantire l'imparzialità del trattamento"[63]. Ad esempio attuando la sorveglianza e l'intervento umani, al fine di attenuare eventuali distorsioni e garantire che non vi sia stigmatizzazione o profilazione dei passeggeri.

A.2.2 Garantire che tutti i trattamenti di dati personali siano trasparenti e che le persone siano consapevoli e abbiano il controllo delle modalità di trattamento dei loro dati per ciascun trattamento[64].

A.2.3 Garantire che siano predisposte misure al fine di rispettare il principio di limitazione della finalità in modo che i dati non siano utilizzati per altre finalità, quali quelli di sicurezza o formazione.

A.2.4 Garantire che non siano acquisiti foto o video, anche se non registrati e trattati, di persone che non hanno acconsentito al riconoscimento facciale mediante misure adeguate (ad esempio utilizzando una profondità di campo e un'area di cattura adeguate per evitare di acquisire immagini di altri passeggeri sullo sfondo o nelle vicinanze, utilizzando file dedicate chiaramente contrassegnate per il riconoscimento facciale).

A.2.5 Se i passeggeri che acconsentono e quelli che non acconsentono al riconoscimento facciale possono utilizzare le medesime postazioni o se i passeggeri che non acconsentono al riconoscimento facciale possono apparire nel campo visivo mentre il sistema non è in uso, attendere un'azione positiva da parte di un passeggero che ha prestato il consenso prima di iniziare l'acquisizione di foto o video.

A.2.6 Possibilità per l'interessato di effettuare in qualsiasi momento la cancellazione dei dati esclusivamente in suo possesso (modello biometrico[65]) contenuti in un'applicazione mobile o in un portafoglio digitale[66].

A.2.7 Esistenza di alternative valide o soluzioni di back-up (ossia per i passeggeri che non acconsentirebbero all'uso dei loro dati biometrici, per i passeggeri che non sarebbero in grado

[63] EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, nota 60, punto 70.
[64] EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, punto 68 e considerando 7 GDPR.
[65] I riferimenti al modello biometrico nelle garanzie per lo scenario 1 corrispondono ai riferimenti alla chiave segreta nello scenario 2.
[66] Si noti che questa garanzia si applica solo allo scenario 1.

di utilizzare tali soluzioni o per i passeggeri oggetto di falsi negativi), in modo da garantire che i passeggeri che non prestano il loro consenso non subiscano pregiudizio[67].

A.2.8 Se si utilizza un'applicazione, questa deve essere attentamente progettata e configurata in modo da non raccogliere dati superflui ed evitare l'uso di kit di sviluppo software (*Software Development Kit*, SDK) di terzi che raccolgono dati per altre finalità.

A.3 Responsabilizzazione

A.3.1 Valutare se esistono codici di condotta o meccanismi di certificazione pertinenti per contribuire a dimostrare la conformità alla sicurezza del trattamento di cui all'articolo 32 GDPR[68]. Verificare l'adeguatezza delle misure con riguardo allo specifico trattamento in questione. Norme[69], migliori prassi e codici di condotta, riconosciuti da associazioni e da altri organismi che rappresentano categorie di titolari del trattamento possono essere utili ai fini della determinazione di misure adeguate.

A.3.2 Garantire l'esecuzione di controlli di sicurezza di base sul dispositivo dell'utente per consentire la fase di registrazione, sebbene anche il passeggero abbia un ruolo nella protezione dei suoi dati in quanto conservati sul proprio dispositivo. Esempi di tali verifiche e controlli tecnici sono presentati di seguito nella sezione C.2 "Infrastruttura e rete".

B. Considerazioni organizzative

B.1 Politica e conformità

B.1.1. Garantire che siano posti in essere controlli interni degli accessi[70] con norme per gli amministratori.

B.1.2 Qualora il servizio di riconoscimento facciale possa essere fornito da una delle parti coinvolte nel trattamento senza che i dati di identificazione o biometrici, o di entrambi i tipi, debbano essere trattati dalle altre parti coinvolte, vietare che tali dati circolino tra dette altre parti. Ad esempio una compagnia aerea non è tenuta ad accedere tecnicamente ai dati biometrici quando si affida all'infrastruttura comune dell'aeroporto, anche se tale compagnia aerea agisce in qualità di titolare del trattamento ai sensi del GDPR.

---

[67] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 86.
[68] Articolo 32, paragrafo 3, GDPR e EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, punto 10.
[69] Cfr. ad esempio ISO/IEC 2382-37.
[70] EDPB, *Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19* (in appresso "**linee guida 04/2020 dell'EDPB sui dati di localizzazione e sugli strumenti per il tracciamento dei contatti**"), SEC-10, pag. 16.

B.1.3 Definire una politica per la cifratura e la gestione delle chiavi[71], ad esempio per il trattamento dei dati di identificazione e dei dati biometrici.

B.1.4 Garantire la conformità al capo V GDPR, ad esempio per garantire trasferimenti conformi se il titolare del trattamento utilizza un servizio a distanza durante il processo di registrazione che ha sede in un paese terzo.

B.1.5 In caso ci si avvalga di responsabili del trattamento, garantire l'esistenza di un contratto con il responsabile del trattamento[72] in linea con l'articolo 28, paragrafo 3, GDPR;

B.1.6 Garantire l'esistenza di procedure per gestire la sorveglianza e l'intervento umani, in particolare per affrontare i problemi legati ai falsi negativi e i problemi tecnici o di usabilità.

B.2 Formazione e test

B.2.1. Garantire che il personale sia adeguatamente formato.

B.2.2 Mettere in atto "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento"[73].

B.2.3. Attuare un processo per garantire che il trattamento del modello biometrico del passeggero[74] ai fini dell'autenticazione sia tecnicamente efficace e sufficientemente accurato.

B.2.4. Garantire che i campioni biometrici raccolti sia al momento della registrazione sia al punto di controllo siano di qualità sufficiente per effettuare un trattamento biometrico affidabile.

C. Considerazioni tecniche

C.1 Accesso

C.1.1 Mettere in atto garanzie durante la fase di registrazione per garantire l'applicazione del metodo di *bootstrapping* al processo di registrazione con un'identità verificata. Ad esempio, per rafforzare la valutazione dell'autenticazione a più fattori per le identità degli utenti, è possibile attuare misure che spaziano dai link una tantum protetti da password per attivare l'applicazione ai meccanismi di sblocco dei dispositivi locali.

[71] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 89.
[72] Articolo 28, paragrafo 3, GDPR.
[73] Articolo 32, paragrafo 1, lettera d), GDPR.
[74] I riferimenti al modello biometrico nelle garanzie per lo scenario 1 corrispondono ai riferimenti alla chiave segreta nello scenario 2.

C.1.2 Mettere in atto garanzie per affrontare i problemi legati ai casi di falsi positivi, agli attacchi di presentazione e alla prevenzione delle frodi[75].

C.1.3 Vietare qualsiasi accesso esterno ai dati di identificazione e ai dati biometrici[76].

C.1.4 Garantire che il trattamento sia effettuato a livello locale nelle fasi di registrazione, trasmissione e confronto. Il punto di confronto deve essere il più vicino possibile al dispositivo della persona. Il confronto del modello all'interno del singolo dispositivo potrebbe richiedere un'interazione con fornitori di servizi situati al di fuori dell'aeroporto e l'utilizzo di risorse di rete pubbliche, con l'inconveniente di compromettere la disponibilità e la diffusione del modello a entità esterne.

C.1.5 Autenticare un utente per aggiungere un nuovo volo e generare un nuovo codice QR cifrato.

C.1.6 Attuare misure per affrontare la situazione in cui un passeggero può perdere l'accesso al proprio codice QR.

C.2 Infrastruttura e rete

C.2.1 Mantenere aggiornate le condizioni relative al sistema operativo ("SO") e consentire l'autenticazione per l'accesso al dispositivo per l'utilizzo dell'applicazione/del portafoglio digitale, anche con cancellazione automatica dei dati di identificazione e dei dati biometrici se il sistema operativo è obsoleto e comporta rischi per la sicurezza.

C.2.2 Isolamento delle unità di confronto (ossia delle postazioni) dalla rete durante il funzionamento e adozione di tutte le altre misure necessarie per garantire la sicurezza.

C.2.3 Effettuare il confronto biometrico sul dispositivo del passeggero o nella postazione (*edge computing*).

C.2.4 Soluzioni per affrontare le vulnerabilità della sicurezza dei singoli dispositivi dei passeggeri, compresa la cifratura (quanto meno) dei dati di identificazione e dei dati biometrici "a riposo".

C.2.5 Utilizzare una conservazione sicura (quanto meno) dei dati biometrici esclusivamente nelle mani dell'utente[77], ad esempio utilizzando un'*enclave* sicura su uno smartphone.

C.2.6 Garanzie di sicurezza per assicurare la sicurezza fisica dei locali, compreso il terminal biometrico dell'aeroporto. Garantire un elevato livello di sicurezza per gli elementi

[75] ENISA, *Digital Identity – Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust,* gennaio 2022.
[76] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 89.
[77] I riferimenti al modello biometrico nelle garanzie per lo scenario 1 corrispondono ai riferimenti alla chiave segreta nello scenario 2.

dell'architettura che trattano (ad esempio calcolo, flusso di dati, conservazione transitoria o a lungo termine) i dati di identificazione e i dati biometrici.

C.3 Sicurezza e gestione dei dati di controllo dell'identità dell'utente

C.3.1 Compartimentalizzare i dati durante la trasmissione e la conservazione in almeno tre gruppi diversi, come ad esempio: dati di identificazione, dati biometrici e informazioni relative al volo[78]. Garantire che i dati siano opportunamente cifrati tra la trasmissione e la conservazione.

C.3.2 Attuare misure tecniche per garantire che solo i dati che possono essere trattati in modo lecito negli specifici punti di controllo siano trattati e verificati in tale punto.

C.3.3 Garantire l'efficacia della cancellazione dei dati[79] mediante una procedura di cancellazione sicura (ad esempio memoria principale, *cache*, potenziali backup) e valutare quando tale cancellazione dovrebbe essere automatizzata. I periodi di conservazione dei dati dovrebbero essere rigorosamente applicati mediante procedure automatiche senza che sia necessaria un'azione supplementare da parte della persona[80].

C.3.4 Garantire l'autenticità e l'integrità dei dati (ad esempio firma)[81].

C.3.5 Conservare i dati biometrici dei passeggeri al punto di registrazione e al punto di controllo solo per un periodo molto breve e cancellarli non appena il passeggero ha attraversato il punto di controllo.

C.3.6 Se un'applicazione è utilizzata per la registrazione, applicare le norme di sicurezza per la sicurezza delle applicazioni mobili durante lo sviluppo dell'applicazione, nonché garantire l'effettuazione di test di sicurezza da parte di terzi.

C.3.7 Garantire l'attuazione di misure di sicurezza durante la fase di registrazione all'aeroporto per mantenere la riservatezza e l'integrità dei dati biometrici del passeggero. Ad esempio, se stampato dal dispositivo, il codice QR non dovrebbe essere visualizzato su tale dispositivo per evitare che un malintenzionato lo fotografi. Nei casi di trasmissione a corto raggio, la trasmissione dovrebbe essere effettuata sulla base del coinvolgimento attivo dell'utente e attraverso un canale che garantisca la prossimità.

C.3.8 I dati che sono noti esclusivamente alla persona[82] dovrebbero essere conservati in un luogo sicuro sul dispositivo della stessa e le eventuali vulnerabilità relative ai sistemi operativi

[78] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 89.
[79] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 89.
[80] EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, punto 82.
[81] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 89.
[82] I riferimenti al modello biometrico nelle garanzie per lo scenario 1 corrispondono ai riferimenti alla chiave segreta nello scenario 2.

del dispositivo devono essere sottoposte alle opportune *patch* di sicurezza. Nel caso di un codice QR stampato, la persona dovrebbe essere informata della natura particolarmente sensibile dei dati in esso contenuti e di ciò che consente di effettuare.

C.3.9 Garantire che la registrazione sia effettuata seguendo adeguate tecniche di verifica dell'identità a distanza[83].

3.2.2 Scenario 2: conservazione centralizzata del modello biometrico registrato in forma cifrata all'interno dell'aeroporto e con una chiave segreta nota esclusivamente ai passeggeri ai fini dell'autenticazione

48. La presente sezione esamina la compatibilità con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR della conservazione centralizzata ai fini dell'autenticazione dei modelli biometrici registrati dei passeggeri in una banca dati centralizzata in forma cifrata e con una chiave segreta nota esclusivamente al passeggero[84] (in appresso "**scenario 2**"). La presente sezione esamina anche le garanzie adeguate per lo scenario 2 alla luce degli articoli 25 e 32 GDPR.

Descrizione dello scenario

49. Nello scenario 2 la registrazione è effettuata una sola volta, per un determinato periodo di validità (ad esempio un anno dopo l'ultimo volo fino alla scadenza della validità del passaporto), a distanza a un livello di garanzia dell'identità adeguato (ad esempio eIDAS) o presso i terminal aeroportuali. La registrazione è controllata dal gestore aeroportuale e consiste nel generare dati di identificazione e dati biometrici cifrati con una chiave segreta.

50. La banca dati è conservata all'interno dei locali dell'aeroporto sotto il controllo del gestore aeroportuale. Le chiavi segrete di cifratura specifiche per ciascuna persona sono conservate solo sul suo dispositivo (ad esempio nell'applicazione mobile del gestore aeroportuale). L'applicazione può generare un codice QR contenente la chiave segreta, che può essere stampato su carta o visualizzato sullo schermo del dispositivo[85]. Inoltre un secondo livello di cifratura[86] è offerto dal gestore aeroportuale con chiavi controllate da quest'ultimo.

51. I passeggeri sono autenticati (confronto 1:1) quando attraversano specifici punti di controllo in aeroporto. I passeggeri che scelgono di passare attraverso i punti di controllo biometrici mostrano il loro codice QR in un'apposita postazione di controllo dotata di scanner QR e di una videocamera. L'impronta dell'indice del passeggero è inviata alla banca dati per richiedere il modello cifrato che è scaricato e controllato localmente sulla postazione e/o sul dispositivo dell'utente. Solo il risultato del confronto è reso noto al titolare del trattamento del punto di controllo e da questi utilizzato[87].

---

[83] Cfr. ENISA, *Remote ID Proofing – Analysis of methods to carry out identity proofing remotely*, marzo 2021.
[84] Come esemplificato dal caso d'uso 2 nell'allegato I della richiesta.
[85] L'AC FR ha ulteriormente chiarito che potrebbero esserci anche altre soluzioni tecniche per inviare le informazioni richieste, ad esempio utilizzando un protocollo di comunicazione a corto raggio.
[86] La chiave segreta (nota alla persona) è a sua volta cifrata con un'altra chiave in possesso del gestore aeroportuale.
[87] L'AC FR ha chiarito che tale periodo di conservazione è indicativo e può essere considerato accettabile, dato che la chiave è nota alle persone e potrebbe essere scelta nella fase di registrazione. È tuttavia opportuno osservare che tale periodo di conservazione può essere adeguato.

52. In questo scenario non vi sono flussi di dati di identificazione e dati biometrici tra gli aeroporti, così come neppure l'interconnessione né l'interoperabilità tra le banche dati centralizzate.

Valutazione dell'EDPB

53. Nello scenario 2 i modelli biometrici registrati dei passeggeri sono conservati in modo centralizzato, ma in forma cifrata e con una chiave segreta nota esclusivamente ai passeggeri. Nello scenario 2 i passeggeri sono autenticati (confronto 1:1).

54. In questo scenario si propone che l'obiettivo di snellire il flusso di passeggeri (ossia aumentando la velocità dei controlli) possa essere conseguito con l'uso di un sistema centralizzato. L'EDPB ha già osservato che tale soluzione potrebbe essere considerata un'alternativa praticabile alla conservazione decentralizzata dei modelli biometrici registrati[88] (come descritto nello scenario 1), se in presenza di esigenze oggettive e con l'utilizzo di garanzie adeguate (cfr. garanzie descritte dal punto 60).

55. In termini di sicurezza, i dati di ciascuna persona sono cifrati con la chiave specifica nota esclusivamente a tale persona e sotto il suo esclusivo controllo. Inoltre il fatto che le informazioni richieste per il confronto (ossia la chiave segreta) debbano essere fornite dalla persona funge da secondo fattore[89] e rafforza quindi la sicurezza dell'autenticazione. Per di più un secondo livello di cifratura è offerto dal gestore aeroportuale con chiavi controllate da quest'ultimo. Nello scenario 2 l'impronta dell'indice della persona è inviata alla banca dati centrale in modo da recuperare i dati biometrici ad essa associati. Tali dati sono quindi inviati (cifrati) a un computer localizzato al punto di controllo dove sono decifrati per effettuare il confronto e solo il risultato di detto confronto è reso noto al titolare del trattamento del punto di controllo e utilizzato dallo stesso. A condizione che la chiave segreta della persona sia conservata nel computer localizzato al punto di controllo e che solo l'impronta dell'indice del passeggero sia inviata alla banca dati centrale per recuperare il modello biometrico cifrato, tali misure di sicurezza potrebbero pertanto essere considerate compatibili con l'articolo 5, paragrafo 1, lettera f), e con l'articolo 32 GDPR.

56. Per quanto riguarda la compatibilità con l'articolo 25 GDPR e in particolare per conformarsi al requisito della minimizzazione dei dati, è opportuno garantire che il trattamento soddisfi il principio di necessità. Nello scenario 2 si potrebbe ritenere che le misure scelte abbiano soddisfatto il principio di necessità in relazione alla finalità perseguita (ossia snellire il flusso dei passeggeri negli aeroporti) se, a seconda delle circostanze del trattamento, il titolare del trattamento può dimostrare che non esistono soluzioni alternative meno invasive in grado di conseguire lo stesso obiettivo in modo altrettanto efficace. Nello scenario 2 i passeggeri dovrebbero comunque mostrare il proprio dispositivo[90]. Tuttavia il titolare del trattamento può essere in grado di dimostrare che lo scenario 2 accelera il processo di verifica rispetto alla situazione attuale, che prevede la verifica umana della corrispondenza tra il nome sulla carta d'imbarco e il documento d'identità del passeggero[91], o rispetto allo scenario 1. In particolare ciò non potrebbe essere dimostrato se attualmente non si effettuano

[88] Linee guida 3/2019 dell'EDPB sui dispositivi video, punto 88.
[89] Ciò attenua ad esempio il rischio di *spoofing* dell'identità. Cfr. anche la garanzia C.1.2.
[90] L'AC FR ha ulteriormente chiarito che potrebbero esserci anche altre opzioni per presentare un modello, ad esempio stampato su carta. Inoltre l'EDPB riconosce che in futuro si potrebbe prevedere l'uso di una tecnologia alternativa, ad esempio basata su un sistema di comunicazione a corto raggio.
[91] Si potrebbe inoltre sostenere che il controllo biometrico può essere meno soggetto ad errori rispetto al controllo umano.

controlli per verificare l'identità dei passeggeri sulla base del loro documento d'identità ufficiale (a tale riguardo cfr. punto 18).

57. Per quanto riguarda il principio di proporzionalità, l'invasività derivante da tale trattamento può essere controbilanciata dal coinvolgimento attivo dei passeggeri, che detengono sotto il loro esclusivo controllo la chiave dei loro dati cifrati. Inoltre sembra che i rischi per la sicurezza derivanti dalla conservazione dei dati biometrici dei passeggeri in una banca dati centralizzata e con la chiave nota esclusivamente ai passeggeri possano essere attenuati ricorrendo a garanzie adeguate (cfr. garanzie esaminate dal punto 60). Pertanto, supponendo che il titolare del trattamento attui garanzie adeguate come richiesto dallo specifico trattamento in questione, i rischi per le persone potrebbero essere attenuati e l'impatto negativo sui diritti e sulle libertà fondamentali degli interessati potrebbe essere considerato proporzionato al vantaggio previsto. Naturalmente in ciascun caso si dovrebbe garantire che siano trattati solo i dati necessari per la finalità e che siano controllati solo i passeggeri che hanno acconsentito, evitando così il rischio che siano raccolti dati biometrici di altri passeggeri che non hanno prestato il loro consenso.

58. Nella richiesta si afferma a titolo esemplificativo che nello scenario 2 il periodo di conservazione dei dati cifrati nella banca dati potrebbe generalmente essere di un anno dopo l'ultimo volo sul quale si è imbarcata la persona e fino alla scadenza della validità del passaporto. Nella richiesta non è stata fornita alcuna informazione per giustificare un periodo così lungo sulla base di ragioni oggettive, sebbene si possa presumere sia previsto tale periodo di conservazione a fini di comodità per i voli futuri. In termini di periodo di conservazione, al fine di conseguire la compatibilità con l'articolo 5, paragrafo 1, lettera e), GDPR in questo scenario, i titolari del trattamento dovrebbero essere in grado di giustificare il motivo per cui tale periodo di conservazione è necessario per la finalità in casi specifici. Il Comitato raccomanda ai titolari del trattamento di prevedere il periodo di conservazione più breve possibile, tenendo conto anche dei passeggeri che volano solo molto raramente, e di offrire agli interessati la possibilità di stabilire il periodo di conservazione che preferiscono.

59. Alla luce di tali considerazioni, in risposta alla domanda 2.1.1, il Comitato conclude che tale trattamento **potrebbe essere considerato in linea di principio compatibile con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR, fatte salve le garanzie adeguate**.

Garanzie adeguate

60. In questo tipo di scenario, in risposta alla domanda 2.1.2, il Comitato ritiene che, **oltre alle garanzie elencate nello scenario 1**, dovrebbero essere attuate almeno le garanzie indicate di seguito. Garanzie diverse da quelle descritte nel presente parere potrebbero essere utilizzate per conseguire gli stessi obiettivi di sicurezza e protezione dei dati e potrebbero essere lecite purché garantiscano la conformità ai quadri giuridici applicabili.

61. Nota: *si tratta di una panoramica di alto livello e non esaustiva delle possibili garanzie adeguate, che potrebbero essere attuate da un titolare del trattamento in una soluzione simile allo scenario 2. La loro adeguatezza ai sensi degli articoli 25 e 32 GDPR dipenderà da un'analisi caso per caso. Tutti i titolari del trattamento dovranno assicurarsi di effettuare la propria DPIA e le loro soluzioni specifiche possono richiedere misure supplementari non incluse nel presente parere.*

D. Considerazioni generali

D.1 Diritti degli interessati e garanzie che possono essere attuate dai titolari del trattamento

D.1.1 Garantire che il passeggero abbia il controllo sui periodi di conservazione di tutti i suoi dati. I periodi di conservazione dovrebbero essere limitati a quanto necessario per la finalità specifica. È opportuno stabilire un periodo massimo a seguito di un'analisi approfondita di fattori quali la validità del documento di identificazione. Agli interessati dovrebbe essere offerta la possibilità di stabilire il periodo di conservazione che preferiscono, che potrebbe essere più breve rispetto a quello predefinito.

D.1.2 Possibilità per l'interessato di richiedere in qualsiasi momento la cancellazione dei dati esclusivamente in suo possesso (chiave segreta) contenuti in un'applicazione mobile o in un portafoglio digitale[92].

D.1.3 Garantire che la localizzazione della banca dati centrale consenta un controllo efficace da parte dell'autorità di controllo competente.

E. Considerazioni organizzative

E.1 Politica e conformità

E.1.1 Il margine di fiducia riservato al server centrale deve essere limitato. Garantire che la gestione del server centrale segua regole di governance chiaramente definite e comprenda tutte le misure necessarie per garantirne la sicurezza[93].

F. Considerazioni tecniche

F.1 Accesso

F.1.1 Conservare le registrazioni di chi ha accesso ai dati personali, in particolare ai dati di identificazione e ai dati biometrici, e del momento in cui sono stati consultati.

F.2 Infrastruttura e rete

F.2.1 Proteggere adeguatamente la banca dati centrale, anche contro gli attacchi alla disponibilità.

F.2.2 Garantire che non vi sia una connessione internet alla banca dati centrale, alle postazioni di registrazione e alle unità di confronto. Il funzionamento e la manutenzione di questi sistemi (ad esempio backup, *patch*, monitoraggio ecc.) devono essere effettuati localmente all'interno dei locali dell'aeroporto.

F.3 Sicurezza e gestione dei dati

F.3.1 Implementare le tecniche più avanzate di crittografia per garantire la sicurezza degli scambi tra l'applicazione e il server centrale[94].

F.3.2 Conservare la singola chiave segreta al livello in cui sarà utilizzata per la decifratura (ossia nella postazione) e utilizzare l'impronta dell'indice solo per recuperare il corrispondente modello biometrico registrato nella banca dati centrale.

F.3.3 Garantire che lo scambio di chiavi segrete tra il dispositivo dell'utente e la postazione protegga la comunicazione da eventuali intercettazioni o trasmissioni a terzi.

F.3.4 Associare l'impronta dell'indice al modello biometrico conservato nella banca dati centrale per consentire l'autenticazione 1:1 e garantire che sia unica e correlata alla persona. Garantire che l'impronta dell'indice non riveli alcuna informazione sui dati di identificazione del passeggero e non sia correlata alla chiave di cifratura.

F.3.5 Autenticare e cifrare adeguatamente qualsiasi trasmissione tra la banca dati centrale e i punti di controllo e collocarla su reti isolate.

F.3.6 Evitare i collegamenti bidirezionali tra insiemi di dati (dati di identificazione e dati biometrici, nonché informazioni relative al volo) e conservare nella banca dati solo i collegamenti unidirezionali pertinenti, ad esempio solo quelli da indice a dati di identificazione, da indice a dati biometrici cifrati e da indice a informazioni relative al volo.

F.3.7 Garantire disposizioni in materia di continuità operativa, ad esempio disponendo di adeguati sistemi di conservazione di backup.

F.3.8 Assicurare che la postazione non conservi le registrazioni dei modelli cifrati o non cifrati.

3.2.3 Conservazione centralizzata dei modelli biometrici registrati ai fini dell'identificazione

62. La presente sezione esamina la compatibilità con l'articolo 5, paragrafo 1, lettere e) e f), e con gli articoli 25 e 32 GDPR della conservazione centralizzata ai fini dell'identificazione dei modelli biometrici registrati dei passeggeri, laddove tali modelli non siano cifrati con una chiave segreta nota esclusivamente ai passeggeri, in due casi d'uso: 1) quando tali modelli sono conservati in una banca dati all'interno dell'aeroporto sotto il controllo del gestore aeroportuale[95] (in appresso "**scenario 3.1**") e 2) quando tali modelli sono conservati nel cloud sotto il controllo della compagnia aerea[96] (in appresso "**scenario 3.2**").

[92] Si noti che questa garanzia si applica solo allo scenario 2.
[93] Linee guida 04/2020 dell'EDPB sui dati di localizzazione e sugli strumenti per il tracciamento dei contatti, PRIV-5, pag. 17.
[94] Linee guida 04/2020 dell'EDPB sui dati di localizzazione e sugli strumenti per il tracciamento dei contatti, SEC-4, pag. 16: "[t]ra gli esempi di tecniche utilizzabili figurano la cifratura simmetrica e asimmetrica, funzioni di *hash*, protocolli PMT (*private membership test*), protocolli PSI (*private set intersection*), filtri di Bloom, *private information retrieval*, cifratura omomorfica".
[95] Come esemplificato dal caso d'uso 3A nell'allegato I della richiesta.
[96] Come esemplificato dal caso d'uso 3B nell'allegato I della richiesta.

63. Il Comitato ritiene che l'uso di dati biometrici ai fini dell'**identificazione** in grandi banche dati centrali interferisca con i diritti fondamentali degli interessati e possa comportare gravi conseguenze per gli stessi[97]. Inoltre l'uso dei dati biometrici dovrebbe essere esaminato anche in relazione alla finalità per la quale sono trattati alla luce dei principi di necessità e proporzionalità[98].

3.2.3.1 Scenario 3.1: conservazione centralizzata in una banca dati all'interno dell'aeroporto, sotto il controllo del gestore aeroportuale

Descrizione dello scenario

64. Nello scenario 3.1 il modello biometrico registrato dei passeggeri è conservato in una banca dati centrale presso i locali dell'aeroporto e sotto il controllo del gestore aeroportuale in forma cifrata. In particolare i dati dei passeggeri sono compartimentati, il che significa che i loro dati di identificazione, il modello biometrico registrato e le informazioni relative al volo sono conservati in tre diverse banche dati. Tali dati sono cifrati con chiavi diverse sia durante la conservazione sia durante la trasmissione ai server che effettuano il confronto, dove sono quindi decifrati dal gestore aeroportuale.

65. I passeggeri devono registrarsi per ciascun volo in un breve periodo prima della loro partenza (ad esempio 48 ore). Tale registrazione può essere effettuata a distanza o presso i terminal aeroportuali a un livello di garanzia dell'identità adeguato (ad esempio eIDAS). In alternativa la registrazione può assumere la stessa forma descritta nello scenario 1, nel qual caso i passeggeri devono inviare i loro dati dai portafogli digitali al sistema aeroportuale entro 48 ore prima della loro partenza.

66. Anche in questo scenario i passeggeri si presentano davanti a un'apposita postazione di controllo dotata di videocamera. Il loro campione biometrico è quindi inviato a un server centrale dell'aeroporto, che effettuerà il confronto dei dati con quelli della banca dati biometrica centrale. In questo modo è possibile identificare il passeggero e controllare se è effettivamente registrato per un volo in partenza (o per il volo in imbarco in caso di controllo all'imbarco). A seconda del punto di controllo, i dati rinviati al titolare del trattamento del punto di controllo richiedente possono essere ridotti al minimo, ad esempio sotto forma di "risposta sì/no" o, se necessario, il risultato stesso del confronto. In questo caso solo il risultato della richiesta è trasmesso al titolare del trattamento del punto di controllo e da questi utilizzato.

67. In particolare in questo scenario sono identificati i passeggeri (confronto 1:N), dove N rappresenta il numero di passeggeri previsto nell'aeroporto in un arco di diversi giorni. Inoltre il confronto biometrico è effettuato solo quando ciascun passeggero si presenta ai punti di controllo predefiniti nell'aeroporto di partenza, tuttavia il trattamento dei dati in sé è effettuato da un server centrale collegato alla banca dati centrale. Il periodo di conservazione in questo scenario è generalmente di 48 ore e i dati sono cancellati al decollo dell'aereo.

[97] Cfr. ad esempio il parere 3/2012 del Gruppo di lavoro articolo 29 sulle tecnologie biometriche, pag. 8. Cfr. anche il punto 26.
[98] Considerando 4 GDPR. Cfr. anche il parere 3/2012 del Gruppo di lavoro articolo 29 sulle tecnologie biometriche, pag. 8.

Valutazione dell'EDPB

68. Come ricordato in precedenza, il trattamento dei dati biometrici comporta maggiori rischi per i diritti e le libertà degli interessati[99]. Pertanto eventuali carenze nella sicurezza dei dati possono avere conseguenze particolarmente gravi per gli interessati[100]. I titolari del trattamento sono tenuti ad attenuare efficacemente tali rischi. Dal momento che in questo scenario l'intera architettura è completamente centralizzata, i passeggeri perdono maggiormente il controllo dei loro dati. Inoltre potrebbe essere maggiore anche il rischio che i dati finiscano per essere trattati per finalità diverse da quella del controllo del flusso dei passeggeri.

69. Alla luce del principio e dei requisiti in materia di sicurezza (articolo 5, paragrafo 1, lettera f), e articolo 32 GDPR), si dovrebbe considerare che la conservazione dei dati di identificazione e dei dati biometrici in banche dati centrali, anche se distinte, può fornire punti di attacco di alto valore e una violazione della riservatezza di tali banche dati può successivamente comportare l'accesso all'intero insieme di dati. Di conseguenza una possibile violazione dei modelli di riconoscimento facciale e dei relativi dati di identificazione può consentire l'identificazione non autorizzata o illecita degli interessati in altri ambienti. Può inoltre, a seconda dei metodi utilizzati ai fini dell'identificazione biometrica, compromettere l'ulteriore uso sicuro dei modelli di riconoscimento facciale come mezzo di identificazione. In tal caso gli effetti della violazione non possono essere attenuati, a differenza del caso di un altro tipo di credenziale (ad esempio *user ID*, *password*) che è possibile modificare[101].

70. Inoltre l'elevata quantità e qualità dei dati di identificazione e dei dati biometrici in possesso del titolare del trattamento li rende un bersaglio di alto valore per gli autori di attacchi, il che comporta, in termini di rischio per la sicurezza, un livello più elevato di probabilità. Per di più le violazioni dei dati potrebbero avere un impatto maggiore in quanto, a causa della conservazione dei dati in un luogo centralizzato, potrebbe essere più facile per gli autori di attacchi accedere ai dati personali relativi a più passeggeri. Pertanto un'eventuale violazione potrebbe esporre un gran numero di interessati a rischi elevati in termini di gravità, ad esempio il furto d'identità su larga scala, che sono estremamente difficili da attenuare.

71. Di conseguenza, per quanto riguarda la compatibilità con l'articolo 5, paragrafo 1, lettera f), e l'articolo 32 GDPR, le misure previste nello scenario 3.1[102], tenendo conto dello stato dell'arte, non sono sufficienti a garantire un livello di sicurezza adeguato al rischio. Su tale base il trattamento nell'ambito dello scenario 3.1 non sarebbe conforme all'articolo 5, paragrafo 1, lettera f), e all'articolo 32 GDPR se un titolare del trattamento si limitasse a tali misure.

72. Alla luce del principio di cui all'articolo 5, paragrafo 1, lettera e), GDPR, in questo scenario il periodo di conservazione dei dati biometrici nella banca dati centrale è generalmente di 48 ore. Tale limitazione della conservazione sembra ridurre in modo significativo i rischi associati alle violazioni dei dati personali. Tuttavia il periodo di conservazione dei dati non è di per sé un fattore decisivo per la compatibilità globale di detta architettura, in quanto tali periodi di conservazione possono essere soggetti a modifiche da parte dei titolari del trattamento. In ogni caso le misure proposte devono

[99] Cfr. punto 26.
[100] *Guidelines on facial recognition, Consultative Committee of Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data*, giugno 2021, pag. 22.
[101] Cfr. a tale proposito il parere 3/2012 del Gruppo di lavoro articolo 29 sulle tecnologie biometriche, pag. 34.
[102] Come descritto ai punti 64-67.

rispettare i requisiti in materia di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita ai sensi dell'articolo 25 GDPR.

73. A differenza degli scenari 1 e 2, in cui i passeggeri sono autenticati, nello scenario 3.1 i passeggeri sono identificati (confronto 1:N), dove N rappresenta il numero di passeggeri previsto nell'aeroporto in un arco di diversi giorni che hanno acconsentito a tale trattamento quando attraversano specifici punti di controllo in aeroporto. Ciò implica la ricerca dei passeggeri all'interno di una banca dati centrale, trattando ogni campione biometrico acquisito per verificare se corrisponde a una persona nota al sistema. A differenza dello scenario 2, nello scenario 3.1 le chiavi non sono note esclusivamente ai passeggeri. Di conseguenza in questo scenario i passeggeri hanno un controllo significativamente inferiore sui loro dati biometrici. Pertanto il trattamento proposto nell'ambito dello scenario 3.1 non può essere compatibile con i requisiti in materia di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita ai sensi dell'articolo 25 GDPR.

74. Alla luce dell'articolo 25 GDPR i titolari del trattamento dovrebbero tenere conto delle tipologie, delle categorie e del livello di dettaglio dei dati personali richiesti per le finalità del trattamento[103]. Le loro scelte nella progettazione dovrebbero tenere conto dei maggiori rischi per i principi di integrità e riservatezza, di minimizzazione dei dati e della limitazione della conservazione connessi alla raccolta di grandi quantità di dati personali dettagliati, rispetto ai minori rischi associati alla raccolta di quantità minori di dati e/o di informazioni meno dettagliate sugli interessati. In ogni caso le impostazioni predefinite non dovrebbero includere la raccolta di dati personali che non sono necessari per la specifica finalità del trattamento. In altre parole, se determinate categorie di dati personali sono superflue o se non sono necessari dati particolareggiati, perché sono sufficienti dati meno granulari, allora quelli in eccesso non dovrebbero essere raccolti. In questo caso, qualora un'altra attuazione del trattamento possa conseguire lo stesso obiettivo e sia disponibile secondo i termini descritti nello scenario 3.1, non è necessario utilizzare la tecnologia di riconoscimento facciale.

75. Per quanto riguarda l'articolo 25 GDPR, un elemento chiave della protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita è rappresentato dall'autonomia dell'interessato. In particolare all'interessato dovrebbe essere garantito il massimo grado possibile di autonomia nel determinare l'utilizzo cui sono sottoposti i suoi dati personali, nonché l'ambito di applicazione e le condizioni di tale utilizzo o trattamento[104]. Nello scenario 1 l'interessato avrebbe autonomia e controllo per quanto riguarda l'uso, la divulgazione e la cancellazione dei propri modelli biometrici e nello scenario 2 manterrebbe un certo controllo per quanto riguarda la divulgazione del proprio modello biometrico, in quanto la chiave segreta di cifratura sarebbe conservata nelle sue mani. Tuttavia nello scenario 3.1 l'interessato dipende pienamente dalle scelte del titolare del trattamento con riguardo al trattamento dei suoi dati biometrici e pertanto non ha alcun controllo diretto sull'uso del proprio modello biometrico.

76. Per quanto riguarda la compatibilità con l'articolo 25 GDPR e in particolare al fine di conformarsi al requisito della minimizzazione dei dati, il trattamento previsto nello scenario 3.1 non può soddisfare

[103] Linee guida 4/2019 dell'EDPB sulla protezione dei dati fin dalla progettazione e per impostazione predefinita, punto 49.
[104] Linee guida 4/2019 dell'EDPB sulla protezione dei dati fin dalla progettazione e per impostazione predefinita, punto 70. Il considerando 7 GDPR chiarisce inoltre che "[è] opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano".

il principio di necessità. Il Comitato ritiene che sia possibile conseguire un risultato analogo per snellire il flusso dei passeggeri negli aeroporti in modo meno invasivo della vita privata. Ad esempio ciò può essere conseguito senza l'uso di dati biometrici (anche se l'esperienza dell'utente sarebbe a questo punto diversa, in quanto l'esibizione della carta d'imbarco e se necessario dei documenti di identificazione ufficiali potrebbe richiedere più tempo). Inoltre altre soluzioni, in particolare quelle basate sulla conservazione dei dati biometrici in un portafoglio locale sul dispositivo della persona o quelle che richiedono la cifratura dei dati con una specifica chiave conservata nel dispositivo della persona, consentono di conseguire gli obiettivi in modo meno invasivo della vita privata.

77. Per quanto riguarda il principio di proporzionalità, il trattamento previsto nello scenario 3.1 comporterebbe rischi per i diritti degli interessati che non sarebbero attenuati dalle garanzie previste tenuto conto dello stato dell'arte. Il rischio di un impatto negativo sui diritti e sulle libertà fondamentali degli interessati che potrebbe derivare da una violazione dei dati in una banca dati centralizzata di dati biometrici di un numero elevato di persone sembra superare il vantaggio previsto derivante dal trattamento, in quanto tale vantaggio è relativamente modesto, ossia un leggero aumento della comodità e della rapidità dei controlli. Pertanto ciò non può giustificare l'elevata invasività di tali misure per i diritti e le libertà fondamentali delle persone e il trattamento previsto nello scenario 3.1 non soddisfa il principio di proporzionalità.

78. Alla luce di tali considerazioni, in risposta alla domanda 2.2.1, il Comitato conclude che, quando il trattamento è effettuato al fine specifico di snellire il flusso dei passeggeri negli aeroporti, il trattamento previsto nello scenario 3.1:

- **non può essere compatibile con l'articolo 25 GDPR**;
- **non sarebbe conforme all'articolo 5, paragrafo 1, lettera f), e all'articolo 32 GDPR** se un titolare del trattamento si limitasse alle misure descritte nello scenario 3.1.

3.2.3.2 Scenario 3.2: conservazione centralizzata in un cloud sotto il controllo della compagnia aerea

Descrizione dello scenario

79. Nello scenario 3.2 il modello biometrico registrato dei passeggeri è conservato nel cloud sotto il controllo della compagnia aerea o del suo fornitore di servizi cloud (responsabile del trattamento). Nella richiesta è specificato che il fornitore di servizi cloud sarebbe situato nel SEE[105]. In questo caso i dati dei passeggeri sono cifrati, ma vengono decifrati quando sono utilizzati (ad esempio quando è effettuata l'operazione di confronto) e le chiavi sono controllate dalla compagnia aerea o dal suo responsabile del trattamento del cloud. I dati biometrici dei passeggeri sono utilizzati per l'identificazione dei passeggeri (confronto 1:N), dove N rappresenta potenzialmente fino al numero totale di clienti della compagnia aerea[106].

[105] L'AC FR ha chiarito che ciò è indicativo e che potrebbero essere presi in considerazione anche fornitori di servizi cloud che non sono situati nel SEE. Inoltre potrebbero essere previste anche altre soluzioni di conservazione (ad esempio senza l'uso del cloud).
[106] L'AC FR ha chiarito che ciò è indicativo e che esiste una soluzione in base alla quale i dati biometrici sono inviati ogni volta prima del volo.

80. Analogamente agli scenari 1, 2 e 3.1, anche in questo caso i passeggeri devono prima registrarsi. Tuttavia nello scenario 3.2 la registrazione dei passeggeri è effettuata una volta e non deve essere ripetuta finché il cliente ha un account presso la compagnia aerea. La registrazione avviene in modalità a distanza a un livello di garanzia dell'identità adeguato (ad esempio eIDAS) o presso i terminal aeroportuali. Il confronto biometrico è effettuato solo quando i passeggeri si presentano ai punti di controllo predefiniti nell'aeroporto, tuttavia il trattamento dei dati in sé è effettuato nel cloud.

81. All'aeroporto i passeggeri passano attraverso apposite postazioni di controllo dotate di videocamera. I dati biometrici dei passeggeri sono inviati tramite una richiesta a un server cloud della compagnia aerea, dove è effettuato il confronto di tali dati rispetto a quelli contenuti nella banca dati centrale. In questo modo è possibile identificare il passeggero e controllare se è effettivamente registrato per un volo in partenza (o per il volo in imbarco in caso di controllo all'imbarco).

82. I risultati del confronto possono essere potenzialmente messi a disposizione di più gestori aeroportuali, qualora una compagnia aerea disponga di un terminal o di un accesso dedicato all'infrastruttura del sistema di informazione comune di un aeroporto. A seconda del punto di controllo, i dati rinviati al titolare del trattamento del punto di controllo richiedente possono essere ridotti al minimo, ad esempio sotto forma di "risposta sì/no" o, se necessario, il risultato stesso del confronto. In questo caso solo il risultato della richiesta è reso noto al titolare del trattamento del punto di controllo e da questi utilizzato.

83. Il periodo di conservazione del modello è definito dalla compagnia aerea e può potenzialmente durare fino a quando il cliente ha un account presso la compagnia aerea.

Valutazione dell'EDPB

84. Le considerazioni già espresse dal Comitato in relazione allo scenario 3.1[107] valgono anche per questo scenario.

85. Per quanto riguarda il principio e i requisiti in materia di sicurezza (articolo 5, paragrafo 1, lettera f), e articolo 32 GDPR), il trattamento nello scenario 3.2 è effettuato nel cloud e più soggetti potrebbero avere accesso a tali dati, compresi eventualmente fornitori non appartenenti al SEE, anche quando i dati sono conservati nel SEE[108]. Tale architettura comporta potenziali rischi per quanto riguarda i trasferimenti dei dati personali verso paesi terzi. Inoltre, sebbene siano cifrati, i dati dei passeggeri sono decifrati quando sono utilizzati (ossia quando è effettuata l'operazione di confronto), mentre le chiavi sono controllate dalla compagnia aerea o dal suo responsabile del trattamento del cloud. Tale conservazione può comportare un ulteriore aumento della superficie di esposizione alla sicurezza.

86. Pertanto, per quanto riguarda la compatibilità con l'articolo 5, paragrafo 1, lettera f), e l'articolo 32 GDPR, le misure previste nello scenario 3.2[109], tenendo conto dello stato dell'arte, non sono sufficienti a garantire un livello di sicurezza adeguato al rischio. Su tale base il trattamento nell'ambito dello scenario 3.2 non sarebbe conforme all'articolo 5, paragrafo 1, lettera f), e all'articolo 32 GDPR se un titolare del trattamento si limitasse a tali misure.

[107] Punti da 68 a 77.
[108] EDPB, *2022 Coordinated Enforcement Action – Use of cloud-based services by the public sector*, 17 gennaio 2023, pag. 19.
[109] Cfr. punti da 79 a 83.

87. Inoltre, secondo lo scenario 3.2[110], i dati potrebbero essere conservati per un periodo significativo (ossia potenzialmente per tutto il tempo in cui l'interessato ha un account presso la compagnia aerea). Tale durata di conservazione espone i dati a maggiori rischi di violazione della loro riservatezza e integrità e sembra andare oltre quanto strettamente necessario e proporzionato ai fini del trattamento. Il Comitato osserva che il periodo di conservazione dei dati non è di per sé un fattore decisivo per la compatibilità globale con il GDPR di detta architettura, in quanto può essere soggetto a modifiche da parte dei titolari del trattamento. Tuttavia, sulla base delle informazioni a disposizione del Comitato e contenute nella descrizione dello scenario 3.2, non vi è una giustificazione sufficiente per tale lungo periodo di conservazione e non sussistono misure evidenti per attenuare i rischi per le persone. Su tale base il periodo di conservazione proposto non sarebbe limitato a quanto necessario, conformemente al principio di limitazione della conservazione di cui all'articolo 5, paragrafo 1, lettera e), GDPR.

88. In ogni caso le misure proposte nello scenario 3.2 non possono soddisfare i requisiti in materia di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita di cui all'articolo 25 GDPR. Nello scenario 3.2 i modelli biometrici registrati dei passeggeri sono conservati nel cloud sotto il controllo della compagnia aerea o del suo fornitore di servizi cloud (responsabile del trattamento). Come descritto in precedenza, più soggetti potrebbero potenzialmente avere accesso a tali dati. Inoltre i dati biometrici dei passeggeri sono utilizzati per l'identificazione dei passeggeri (confronto 1:N), dove N rappresenta potenzialmente fino al numero totale di utenti/clienti della compagnia aerea. Tale metodo consiste nel trovare una persona tra un gruppo di persone all'interno della banca dati centrale, trattando ogni volto acquisito per verificare se corrisponde a una persona nota al sistema. A differenza dello scenario 3.1, nello scenario 3.2 il confronto potrebbe essere effettuato su scala molto più ampia, in quanto il criterio è in questo caso il numero di clienti totali della compagnia aerea, mentre nello scenario 3.1 si teneva conto solo del numero di passeggeri previsti in un arco di diversi giorni.

89. Inoltre, per quanto riguarda la compatibilità con l'articolo 25 GDPR e in particolare al fine di conformarsi al requisito della minimizzazione dei dati, il trattamento previsto nello scenario 3.2 non può soddisfare il principio di necessità. Il Comitato ritiene che sia possibile conseguire un risultato analogo per snellire il flusso dei passeggeri negli aeroporti ricorrendo a misure meno invasive, ad esempio senza l'uso di dati biometrici, anche se l'esperienza dell'utente sarebbe diversa in quanto l'esibizione del suo documento di identificazione e della sua carta d'imbarco potrebbe richiedere più tempo. Inoltre altre soluzioni, in particolare quelle basate sulla conservazione dei dati biometrici in un portafoglio locale sul dispositivo della persona o quelle che richiedono la cifratura dei dati con una specifica chiave conservata nel dispositivo della persona, consentono al titolare del trattamento di conseguire gli obiettivi in modo meno invasivo della vita privata.

90. Per quanto riguarda il principio di proporzionalità, il trattamento previsto nello scenario 3.2 comporterebbe rischi per i diritti degli interessati che non sarebbero attenuati dalle garanzie previste. L'impatto negativo sui diritti e sulle libertà fondamentali degli interessati che deriverebbe da una violazione dei dati in una banca dati centralizzata di dati biometrici di un numero elevato di persone conservati nel cloud sembra superare il vantaggio previsto derivante dal trattamento, in quanto tale vantaggio è relativamente modesto, ossia un leggero aumento della comodità e della rapidità dei

[110] Cfr. punto 83.

controlli. Pertanto ciò non può giustificare l'elevata invasività di tali misure per i diritti e le libertà fondamentali delle persone e il trattamento previsto nello scenario 3.2 non può essere considerato proporzionato.

91. Alla luce di tali considerazioni, in risposta alla domanda 2.3.1, il Comitato conclude che, quando il trattamento è effettuato al fine specifico di snellire il flusso dei passeggeri negli aeroporti, il trattamento previsto nello scenario 3.2:

- **non può essere compatibile con l'articolo 25 GDPR**;
- **non sarebbe conforme all'articolo 5, paragrafo 1, lettera f), e all'articolo 32 GDPR** se un titolare del trattamento si limitasse alle misure descritte nello scenario 3.2;
- **non sarebbe conforme all'articolo 5, paragrafo 1, lettera e), GDPR**, in quanto non vi è una giustificazione sufficiente per il periodo di conservazione previsto nello scenario 3.2 sulla base delle informazioni a disposizione del Comitato. Al fine di soddisfare il principio della limitazione della conservazione di cui all'articolo 5, paragrafo 1, lettera e), GDPR, il titolare del trattamento dovrebbe dimostrare che i dati personali non sono conservati più di quanto necessario per le finalità per le quali sono trattati.

4 CONCLUSIONI

92. Per quanto riguarda la domanda 1.1, sulla base della richiesta di un parere da parte dell'AC FR, in relazione ai requisiti di cui all'articolo 5, paragrafo 1), lettera f), e agli articoli 25 e 32 GDPR, e sulla base dell'analisi di cui sopra, il Comitato conclude che:

93. l'uso della tecnologia di riconoscimento facciale per l'autenticazione biometrica al fine specifico di snellire il flusso dei passeggeri negli aeroporti (punti di controllo di sicurezza, consegna dei bagagli, imbarco e accesso alla sala d'attesa per i passeggeri) potrebbe essere considerato in linea di principio compatibile con i principi di integrità e riservatezza di cui all'articolo 5, paragrafo 1, lettera f), e con gli articoli 25 e 32 GDPR nel caso di un'architettura di conservazione, in cui il modello biometrico registrato di ciascun passeggero è conservato localmente sul suo singolo dispositivo e sotto il suo esclusivo controllo, fatte salve le garanzie adeguate descritte dal punto 46.

94. Per quanto riguarda la domanda 2.1.1, sulla base della richiesta di un parere da parte dell'AC FR, in relazione ai requisiti di cui all'articolo 5, paragrafo 1, lettere e) e f), e agli articoli 25 e 32 GDPR, e sulla base dell'analisi di cui sopra, il Comitato conclude che:

95. l'uso della tecnologia di riconoscimento facciale per l'autenticazione biometrica al fine specifico di snellire il flusso dei passeggeri negli aeroporti (punti di controllo di sicurezza, consegna dei bagagli, imbarco e accesso alla sala d'attesa per i passeggeri) potrebbe essere considerato compatibile in linea di principio con il principio della limitazione della conservazione di cui all'articolo 5, paragrafo 1, lettera e), con i principi di integrità e riservatezza di cui all'articolo 5, paragrafo 1, lettera f), e con gli articoli 25 e 32 GDPR nel caso di un'architettura di conservazione centralizzata, in cui il modello biometrico registrato di ciascun passeggero è conservato in una banca dati centrale all'interno dell'aeroporto sotto il controllo del gestore aeroportuale in forma cifrata con una chiave segreta nota esclusivamente alla persona, fatte salve le garanzie adeguate descritte dal punto 60.

96. Per quanto riguarda la domanda 2.2.1, sulla base della richiesta di un parere da parte dell'AC FR, in relazione ai requisiti di cui all'articolo 5, paragrafo 1, lettere e) e f), e agli articoli 25 e 32, GDPR, e sulla base dell'analisi di cui sopra, il Comitato conclude che:

97. l'uso della tecnologia di riconoscimento facciale per l'identificazione biometrica al fine specifico di snellire il flusso dei passeggeri negli aeroporti (punti di controllo di sicurezza, consegna dei bagagli, imbarco e accesso alla sala d'attesa per i passeggeri) nel caso di un'architettura di conservazione centralizzata, laddove i modelli biometrici registrati dei passeggeri non sono cifrati con una chiave segreta nota esclusivamente a ciascun passeggero e sono conservati in una banca dati all'interno dell'aeroporto (sotto il controllo del gestore aeroportuale), non può essere compatibile con l'articolo 25 GDPR. Inoltre tale trattamento non sarebbe conforme al principio di integrità e riservatezza di cui all'articolo 5, paragrafo 1, lettera f), e all'articolo 32 GDPR, se un titolare del trattamento si limitasse alle misure descritte nello scenario 3.1.

98. Per quanto riguarda la domanda 2.3.1, sulla base della richiesta di un parere da parte dell'AC FR, in relazione ai requisiti di cui all'articolo 5, paragrafo 1, lettere e) e f), e agli articoli 25 e 32, GDPR, e sulla base dell'analisi di cui sopra, il Comitato conclude che:

99. l'uso della tecnologia di riconoscimento facciale per l'identificazione biometrica al fine specifico di snellire il flusso dei passeggeri negli aeroporti (punti di controllo di sicurezza, consegna dei bagagli, imbarco e accesso alla sala d'attesa per i passeggeri) nel caso di un'architettura di conservazione centralizzata, laddove i modelli biometrici registrati dei passeggeri non sono cifrati con una chiave segreta nota esclusivamente a ciascun passeggero e sono conservati nel cloud (sotto il controllo della compagnia aerea), non può essere compatibile con l'articolo 25 GDPR. Inoltre tale trattamento non sarebbe conforme ai principi di integrità e riservatezza di cui all'articolo 5, paragrafo 1, lettera f), e all'articolo 32 GDPR, se un titolare del trattamento si limitasse alle misure descritte nello scenario 3.2. Infine, sulla base della descrizione dello scenario 3.2 e delle informazioni a disposizione del Comitato, il trattamento non sarebbe conforme al principio della limitazione della conservazione di cui all'articolo 5, paragrafo 1, lettera e), GDPR.

Per il Comitato europeo per la protezione dei dati

La presidente

(Anu Talus)