Provvedimento del 12 marzo 2026 [10238246]

VEDI ANCHE Newsletter del 15 aprile 2026

[doc. web n. 10238246]

Provvedimento del 12 marzo 2026

Registro dei provvedimenti
n. 164 del 12 marzo 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia, componente, e il dott. Claudio Filippi, vice segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito "Regolamento");

VISTO il d.lgs. del 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice") come novellato dal d.lgs. del 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679";

VISTO il procedimento avviato d'ufficio dal Garante, nei confronti di Società per Azioni Esercizi Aeroportuali S.E.A. (di seguito "SEA"), in ordine al trattamento dei dati biometrici dei passeggeri effettuato per il tramite di un sistema di riconoscimento facciale, denominato "FaceBoarding", ai fini dell'identificazione degli stessi ai varchi di accesso all'area sterile e ai gate di imbarco presso l'aeroporto di Milano Linate;

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Pasquale Stanzione;

PREMESSO

1. Premessa

Con nota del 3 maggio 2024, la Società per Azioni Esercizi Aeroportuali S.E.A. (di seguito "SEA") ha comunicato alla scrivente Autorità di essere in procinto di avviare un'iniziativa concernente l'installazione di un sistema di riconoscimento facciale, denominato "FaceBoarding" presso l'aeroporto di Milano Linate.

La stessa ha, al contempo, rappresentato che l'utilizzo dello stesso era finalizzato all'identificazione dei passeggeri ai varchi di accesso all'area sterile e ai gate di imbarco ubicati

nelle aree aeroportuali.

2. L'Opinion n. 11/2024 adottata il 24 maggio 2024 dal Comitato europeo per la protezione dei dati.

Con riferimento a tale specifica tematica, si è espresso, in data 24 maggio 2024, il Comitato europeo per la protezione dei dati (di seguito anche "Comitato" o "EDPB"), approvando, ai sensi dell'articolo 64, par. 3 del Regolamento, un parere denominato "Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR)" - di seguito "Opinion 11/2024".

Come noto, l'art. 64, par. 3 del Regolamento prevede il potere dell'EDPB di esprimersi, su una questione di applicazione generale del Regolamento, al fine di garantire l'applicazione coerente dello stesso nel SEE (v., in merito, l'art. 65, par. 1, lett. c), del Regolamento).

La sopra citata Opinion 11/2024 riporta, pertanto, nel settore ivi individuato, la posizione del Comitato in ordine alla legittimità, rispetto alle disposizioni di cui agli artt. 5, paragrafo 1, lett. f), 25 e 32 del Regolamento, del trattamento dei dati biometrici dei passeggeri, posto in essere, mediante sistemi di riconoscimento facciale, con la finalità di facilitare le operazioni di accesso dei predetti passeggeri nelle aree aeroportuali.

Sul punto, nel predetto parere, l'EDPB individua alcuni scenari predefiniti, come descritti nella sez. 3.2 dell'Opinion 11/2024, statuendo la conformità del sopra menzionato trattamento, soltanto qualora si configurino le ipotesi denominate "Scenario 1 -conservazione del modello biometrico registrato solo nelle mani della persona ai fini dell'autenticazione" (v. sez. 3.2.1 dell'Opinion n. 11/2024) e "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" (v. sez. 3.2.2 dell'Opinion 11/2024).

Il Comitato rileva, di contro, la non conformità, con la normativa europea di protezione dei dati, dei trattamenti effettuati nel contesto degli altri due scenari ivi contemplati, denominati rispettivamente "Scenario 3.1.- conservazione centralizzata dei modelli biometrici in una banca dati all'interno dell'aeroporto, sotto il controllo del gestore aeroportuale" (v. sez. 3.2.3.1 dell'Opinion 11/2024) e "Scenario 3.2 - conservazione centralizzata dei modelli biometrici in un cloud sotto il controllo della compagnia aerea" (v. sez. 3.2.3.2 dell'Opinion 11/2024).

Con particolare riferimento allo Scenario 3.1., l'Opinion 11/2024 evidenzia, nello specifico, l'illiceità dei trattamenti di dati biometrici, posti in essere mediante sistemi di riconoscimento facciale, che si basino sulla "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", che "siano conservati in una banca dati all'interno dell'aeroporto sotto il controllo del gestore aeroportuale" (v. par. 62-66 dell'Opinion 11/2024).

Tali caratteristiche del trattamento, infatti, da una parte, comportano che gli interessati non siano in grado di esercitare un controllo attivo sulle loro informazioni personali e, dall'altra, determinano una maggiore esposizione del sistema ad attacchi e violazioni dei dati (Opinion 11/2024, paragrafi nn. 68-70).

L'EDPB osserva, invero, che "la conservazione dei dati [personali del passeggero, ivi inclusi quelli 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 degli [ulteriori dati personali dell'interessato] può consentire l'identificazione non autorizzata o illecita" degli stessi per altre finalità (v. Opinion 11/2024, par. 69).

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” (v. Opinion 11/2024, par. 70).

In ragione di quanto sopra, ne consegue la violazione dell’art. 5, paragrafo 1, lettera f), e dell’articolo 32 del Regolamento (v. Opinion 11/2024, par. 71).

L’EDPB ritiene altresì che “a differenza degli Scenari 1 e 2, in cui i passeggeri sono autenticati, nello Scenario 3.1. i passeggeri sono identificati (confronto 1:N)”. 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 – “che prevede la conservazione centralizzata all’interno dell’aeroporto di un modello biometrico registrato in forma cifrata con una chiave segreta nota esclusivamente al passeggero” (Opinion 11/2024, pag. 3) – “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” (v. Opinion 11/2024, par. 73).

Un “elemento chiave della protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita è, [infatti,] 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. (..) Nello Scenario 3.1. [invece] 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” (v. Opinion 11/2024, par. 75).

Su tale base, il Comitato conclude che il trattamento previsto nello Scenario 3.1. non può essere compatibile con l'articolo 25 del Regolamento (v. Opinion 11/2024, par. 78).

3. L’attività istruttoria.

A seguito di quanto comunicato da SEA con la nota del 3 maggio 2024 e tenuto conto del predetto Parere, la scrivente Autorità ha avviato d’ufficio, il 16 dicembre 2024, un’istruttoria volta a verificare in quale degli scenari individuati nell’Opinion 11/2024, potesse essere riconducibile il sistema FaceBoarding operativo presso l’aeroporto di Milano Linate.

3.1. La richiesta di informazioni nei confronti di SEA.

In data 16 dicembre 2024, la scrivente Autorità ha innanzitutto inviato una richiesta di informazioni, a cui la Società ha fornito riscontro, con nota del 14 febbraio 2025 e con successiva comunicazione integrativa del 14 aprile 2025, rappresentando quanto di seguito riportato.

Il FaceBoarding riguarda l’accesso dei passeggeri a due distinte aree aeroportuali: l’area ove vengono effettuati i controlli all’ingresso dell’aeroporto (c.d. “area sterile”) e quella prospiciente il gate di imbarco (v. nota del 14 febbraio 2025, pag. 1).

Il principale obiettivo del sistema è quello di garantire un maggiore livello di sicurezza dei controlli in termini di affidabilità dell’identificazione dei passeggeri.

Il FaceBoarding, inoltre, consente di velocizzare l'accesso all'area sterile e il passaggio al gate, determinando al contempo un incremento del grado di soddisfazione degli utenti in ragione di un generale miglioramento dei servizi presso l'aeroporto (v. nota del 14 febbraio 2025, pag. 2).

Dal punto di vista operativo, è prevista una fase di iscrizione da parte del passeggero (c.d. enrollment), che può avere luogo, sia mediante l'utilizzo di appositi apparati (c.d. chioschi), ubicati presso aree aeroportuali dedicate, sia per il tramite di un'applicazione mobile (di seguito "App"), installata direttamente dall'interessato sul proprio dispositivo mobile personale.

In tale contesto, è inoltre riconosciuta al passeggero la facoltà di optare, previo rilascio di uno specifico consenso, per un programma che comporta la conservazione dei dati fino al 31 dicembre dell'anno di adesione, denominato "Programma a lungo termine" (v. nota del 14 febbraio 2025, pagg. 4 e 5).

La Società ha inoltre dichiarato che, nella fase di enrollment, "quando il passeggero si registra con successo al FaceBoarding tramite i chioschi in aeroporto, S.E.A. crea un token elettronico che associa i dati del documento d'identità, della carta d'imbarco e del template appartenenti al singolo passeggero". Qualora, invece, il passeggero utilizzi l'App, "i dati del documento d'identità, la foto del passeggero e il template del passeggero vengono tra loro associati creando le c.d. Digital Travel Credentials [di seguito anche "DTC"]" (v. nota del 14 febbraio 2025, pag. 3).

In merito, poi, alla compatibilità del FaceBoarding con l'Opinion 11/2024, la Società ha puntualizzato che, sebbene tale sistema presenti "alcune analogie con lo Scenario 3.1., di cui alla sezione 3.2.3.1 dell'Opinion ("Scenario 3.1."), in termini di struttura dei database e di identificazione 1:N", lo stesso tuttavia "non può ritenersi pienamente riconducibile a tale Scenario 3.1. (e a nessun altro degli scenari dell'Opinion)". Tutto ciò in ragione delle specificità che lo contraddistinguono, correlate "soprattutto (..) alle modalità del trattamento del dato biometrico e (..) al livello di controllo assicurato al passeggero sui propri dati personali" (v. nota del 14 febbraio 2025, pag. 3).

Invero, "S.E.A. ha inteso garantire ai passeggeri un controllo significativo sui propri dati personali e assicurare un'elevata mitigazione dei rischi connessi all'eventuale violazione degli stessi. A tal fine, (..) ha implementato specifiche misure che differenziano il FaceBoarding dalla ricostruzione dello Scenario 3.1." dell'Opinion 11/2024 (v. nota del 14 febbraio 2025, pagg. 3 e 5).

Trattasi, nello specifico, delle misure volte a:

> prevedere la conservazione dei dati anagrafici contenuti nel documento di identità e di quelli presenti nel template "in banche dati fisicamente distinte" utilizzando "chiavi diverse di criptazione per i database che contengono i dati dei documenti di identità e di carta d'imbarco". Da ciò ne consegue che "il sistema di S.E.A. è strutturato in maniera tale da mitigare al massimo (se non eliminare del tutto) la probabilità che i dati anagrafici, relativi al documento di identità, possano essere ricollegati al template delle immagini del volto dei passeggeri" (v. nota del 14 febbraio 2025, pag. 6);
>
> prevenire "il rischio di eventi avversi che interessino i dati personali relativi alle caratteristiche del volto dei passeggeri. Questi, infatti, [qualora la registrazione avvenga presso i chioschi] non vengono in nessun caso memorizzati, ma sono trattati soltanto al fine dell'elaborazione del template e poi immediatamente cancellati. (..) In caso di registrazione attraverso App, la foto scattata viene conservata esclusivamente nel dispositivo mobile del passeggero, protetta da codice PIN e ulteriori misure di sicurezza" (v. nota del 14 febbraio 2025, pag. 6);
>
> adottare le c.d. Digital Travel Credentials nell'ambito del funzionamento dell'App. Quest'ultime sono salvate unicamente nel dispositivo del passeggero. SEA non ha, pertanto,

"modo di accedere, modificare, né decriptare le Digital Travel Credentials, che sono trasferite ai sistemi S.E.A. per consentire l'identificazione presso l'aeroporto solo a seguito di un'azione da parte del passeggero in tal senso" (v. nota del 14 febbraio 2025, pag. 4).

In sintesi, la Società "ritiene che il FaceBoarding presenti delle analogie con lo Scenario 3.1. [dell'Opinion n. 11/2024], principalmente in termini di architettura del sistema, ma che sussistano delle specificità del FaceBoarding che ne mitigano fortemente i rischi per i diritti e le libertà del passeggero, allontanando in parte il FaceBoarding dallo stesso Scenario 3.1. Infatti, il passeggero ha un elevato controllo sulla propria identità biometrica" (v. nota del 14 febbraio 2025, pag. 7).

3.2. Gli accertamenti ispettivi effettuati presso la Società.

In ragione di quanto sopra dichiarato da SEA, in data 7 e 8 luglio 2025 è stato effettuato, dall'Autorità, un accertamento ispettivo presso la sede della Società, al fine di valutare più precisamente le caratteristiche e le modalità del funzionamento del sistema.

Dalle verifiche in loco e dall'esame della successiva nota di SEA del 31 luglio 2025, è emerso che:

- il FaceBoarding implementato in via definitiva a far data dal 7 maggio 2024 "interessa i voli operati (sia sulle tratte Schengen sia rispetto a quelle extra Schengen) dalle compagnie aeree ITA Airways e Scandinavian Airlines. Ad oggi i varchi per l'accesso all'area sterile presso i quali è possibile usufruire del sistema sono nel numero di 3 (su 12 varchi complessivi), di cui uno dedicato al Fast track". La registrazione al sistema "può avvenire sia tramite chiosco sia tramite App, e (..), in entrambe le ipotesi, è prevista una fase di enrollment che comporta la scansione di un documento di identità (nella fattispecie, carta di identità elettronica o passaporto elettronico), del volto del passeggero e quella della carta di imbarco". A seguire, "quando il passeggero prova ad attraversare i varchi sopra indicati, viene acquisita l'immagine del volto [di quest'ultimo] che viene trasformata in template biometrico. L'immagine è immediatamente cancellata e il relativo template è utilizzato dal sistema SEA per il confronto biometrico. In caso di esito negativo del confronto, il template viene cancellato sia dal sistema sia dai controller di varco (v. verbale del 7 luglio 2025, pagg. 3 e 4);

- il template è interamente conservato nel sistema centralizzato di SEA; ciò sia con riferimento all'ipotesi in cui la fase di adesione avvenga in aeroporto, per il tramite dei chioschi ivi situati, sia ove la stessa sia effettuata mediante l'App. In particolare, rispetto a quest'ultima ipotesi, è stato verificato che, all'interno delle DTC presenti nell'App, sono memorizzate soltanto le informazioni contenute nel documento d'identità (numero, tipo, data di scadenza, data di nascita, nome e cognome, nazionalità) e "l'immagine del volto dell'interessato acquisita tramite selfie"; mentre "il template biometrico resta conservato esclusivamente nel sistema centralizzato della Società" (v. verbale dell'8 luglio 2025, pag. 2);

- diversamente da quanto constatato in ordine alle modalità di conservazione del template (v. supra), l'informativa, rilasciata da SEA agli interessati al momento della registrazione al sistema, ai sensi dell'art. 13 del Regolamento, riporta che, rispetto alle modalità di adesione al FaceBoarding tramite l'App dedicata, "il modello biometrico (..) resta conservato esclusivamente [nello] smartphone" del passeggero (v. Informativa Privacy FaceBoarding di SEA, punto 7.A., sezione "Registrazione per il singolo volo tramite App"; cfr. anche verbale dell'8 luglio 2025, pag. 2);

- "i dati di enrollment vengono conservati, nei sistemi SEA, in 3 diverse istanze di database che memorizzano, rispettivamente, il template biometrico, i dati delle DTC e i dati della carta di imbarco". In particolare, i dati contenuti all'interno delle Digital Travel Credentials e quelli della carta di imbarco "sono cifrati con chiave AES 256, modificata su base settimanale,

mentre i dati del template sono conservati in chiaro" (v. verbale del 7 luglio 2025, pag. 6);

- rispetto ai tempi di conservazione, quest'ultimi "dipendono dalla scelta effettuata dai passeggeri in fase di enrollment. In caso di scelta relativa all'adesione al servizio per il solo volo, i dati sono cancellati 24 ore dopo il decollo dello stesso, anche al fine di gestire eventuali reclami da parte del passeggero. In caso di adesione [del passeggero al "Programma a lungo termine"], i dati sono conservati per tutto l'anno solare di riferimento, al momento individuato al 31 dicembre 2025" (v. verbale del 7 luglio 2025, pag. 6);

- i tre varchi sopra citati dedicati al FaceBoarding per l'accesso all'area sterile "sono di natura "ibrida" dato che possono essere utilizzati anche dai passeggeri che non hanno aderito al sistema FaceBoarding". In tale specifica circostanza, la cancellazione dei dati dei passeggeri che non hanno effettuato l'enrollment, "avviene di regola entro pochi secondi dalla creazione del template o dall'acquisizione dell'immagine" (v. verbale del 7 luglio 2025, pagg. 3 e 4);

- il numero di passeggeri che hanno viaggiato sulle tratte interessate dal sistema, a partire da maggio 2025 sino alla data dell'accertamento ispettivo, è stato di 3.288.744. Tra questi, "il numero totale di [quelli] che hanno aderito al FaceBoarding (sia al programma lungo che al programma breve, ovvero per singolo volo) [è di] n. 24.550. In particolare, (..) 22.212 passeggeri hanno aderito al programma lungo e (..) 2.338 passeggeri hanno aderito al programma breve (singolo volo)" (v. nota della Società del 31 luglio 2025, pag. 2).

Preso atto di quanto sopra, l'Autorità -ritenuto che il sistema FaceBoarding così concepito rientrasse nello Scenario 3.1. di cui all'Opinion 11/2024 e che il trattamento posto in essere dalla Società fosse in violazione degli artt. 5, par. 1, lettere e) ed f), 6, 13, 25 e 32 del Regolamento- ha ravvisato la necessità di intervenire urgentemente per tutelare i diritti e le libertà degli interessati.

È stato pertanto adottato, l'11 settembre 2025, ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, il provvedimento n. 489, recante la misura della limitazione provvisoria del trattamento dei dati biometrici effettuato da SEA per il tramite del FaceBoarding.

3.3. La notifica delle violazioni.

Con la nota del 7 novembre 2025 l'Autorità, nell'avviare un formale procedimento nei confronti della Società, ha contestato a quest'ultima, ai sensi dell'art. 166, comma 5, del Codice, la violazione dell'art. 5, paragrafo 1, lettere a), e) ed f), e degli articoli 6, 13, 25 e 32 del Regolamento.

La Società ha presentato le proprie memorie difensive il 5 dicembre 2025, rilevando quanto di seguito riportato:

a) con riferimento alle tempistiche dell'istruttoria avviata dal Garante, ha evidenziato che l'Autorità aveva avuto notizia, già nel dicembre 2019, dell'iniziativa di SEA inerente al sistema FaceBoarding a suo tempo assunta nell'ambito di un progetto sperimentale avviato da quest'ultima presso l'aeroporto di Milano Linate. Il predetto sistema era stato oggetto di accertamento ispettivo il 5 e 6 giugno 2023; accertamento a seguito del quale "il Garante non aveva rilevato un quadro di non conformità del progetto", rafforzando pertanto la convinzione di SEA circa la compatibilità dello stesso con la normativa vigente (v. nota della Società del 5 dicembre 2025, pagg. 3-4);

b) con riferimento alla contestata violazione dell'art. 32 del Regolamento rispetto all'assenza di cifratura dei template biometrici conservati sui server della Società, SEA ha ribadito di aver effettuato, prima di avviare le attività di trattamento, una valutazione tecnica, documentata nella DPIA, alla luce della quale "l'approccio di sicurezza stratificato"

implementato dalla Società era stato ritenuto adeguato ai rischi del trattamento; ciò in ragione dell'implementazione di misure di "segregazione fisica dei tre database su server separati con firewall dedicati e controlli di accesso indipendenti", nonchè di un sistema di "cifratura robusta (AES-256) dei database [inerenti alle] DTC e [alle] boarding pass" (v. nota della Società del 5 dicembre 2025, pagg. 8 e 9);

c) in ordine alla presunta violazione dell'art. 6 del Regolamento rispetto ai passeggeri non aderenti al sistema che attraversassero i varchi ibridi, la Società ha evidenziato che questi ultimi "erano chiaramente identificati (..) con apposita cartellonistica dedicata (..) che segnalava (..) il fatto che il passaggio attraverso tali varchi avrebbe potuto comportare un trattamento biometrico. Tale informazione era idonea a creare una aspettativa consapevole nell'utente circa la natura del trattamento, in coerenza con il principio di trasparenza (art. 13 GDPR)". Ha rilevato altresì che "per i passeggeri non iscritti al servizio, il template biometrico veniva cancellato automaticamente e in un lasso temporale inferiore a 1,5 secondi dal rilevamento, senza alcuna ulteriore elaborazione o conservazione". SEA ha inoltre apposto, successivamente, "una cartellonistica aggiuntiva e predisposto informative multicanale (App, sito web, chioschi) per garantire la massima chiarezza" (v. nota della Società del 5 dicembre 2025, pag. 12).

La Società ha inoltre precisato che la durata del trattamento è stata di "circa 1 anno 4 mesi" –ovvero "dal 7 maggio 2024 al 16 settembre 2025" e che il numero di interessati coinvolti fino al 31 luglio 2025 (ossia "24.550 utenti su 3.288.744 passeggeri totali") corrisponde esclusivamente allo "0,75% del traffico passeggeri complessivo in quell'arco temporale" (v. nota della Società del 5 dicembre 2025, pag. 13).

Da ultimo, SEA ha informato l'Autorità di aver adottato "tempestivamente misure concrete per attenuare qualsiasi potenziale danno agli interessati", già "immediatamente dopo l'ispezione del luglio 2025 e prima della notifica formale della violazione (avvenuta il 7 novembre 2025)".

Si tratta di misure consistenti nello specifico in: "implementazione della cifratura AES-256 anche del database contenente i template biometrici (con automatica cifratura dei template in esso conservati) eseguita il 9 settembre 2025 subito dopo l'ispezione dello scorso luglio; sospensione immediata del servizio FaceBoarding in ottemperanza all'ordine del Garante dell'11 settembre 2025 (notificato a SEA il 16 settembre scorso); cancellazione completa e irreversibile di tutti i dati biometrici ed anagrafici all'8 ottobre 2025; revisione e aggiornamento dell'informativa privacy" (v. nota della Società del 5 dicembre 2025, pagg. 10, 11, 14 e 17).

4. Le valutazioni dell'Autorità.

In primis, si rappresenta che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante".

Alla luce degli elementi acquisiti nell'ambito del procedimento, emergono, a carico di SEA, i profili di violazione di seguito esplicitati.

Dall'analisi delle caratteristiche tecniche e delle modalità di funzionamento del sistema FaceBoarding, si rileva innanzi tutto che lo stesso prevede la memorizzazione dei template biometrici dei passeggeri in un archivio centralizzato presso il gestore aeroportuale; ciò senza garantire al contempo ai predetti interessati come richiesto dall'EDPB nell'Opinion 11/2024 un potere di controllo esclusivo sui propri dati biometrici.

Il FaceBoarding risulta pertanto pienamente riconducibile allo Scenario 3.1. della predetta Opinion

e, in quanto tale, si pone in violazione dell'art. 5, paragrafo 1, lett. f), e degli articoli 25 e 32 Regolamento (cfr. sez. 3.2.3.1 dell'Opinion 11/2024 e, più nel dettaglio, quanto richiamato ai paragrafi 3.1. e 3.2 della presente decisione).

Il predetto sistema, infatti, prevede che il modello biometrico del passeggero sia interamente conservato in maniera centralizzata nei server di SEA, in assenza di misure volte a consentire all'interessato di esercitare un controllo esclusivo sui propri dati biometrici; ciò sia con riferimento all'ipotesi in cui la fase di registrazione avvenga in aeroporto, per il tramite dei chioschi ivi ubicati, sia ove la stessa venga effettuata mediante l'App.

In particolare, qualora il trattamento sia posto in essere mediante l'utilizzo dell'applicazione mobile, è stato verificato che diversamente da quanto rappresentato dalla Società in prima battuta con nota del 14 febbraio 2025 (v. supra, paragrafi 3.1 e 3.2.) i modelli biometrici sono conservati in modo centralizzato all'interno di una banca dati presso i sistemi di SEA, sotto il controllo di quest'ultima.

Le Digital Travel Credentials, infatti, salvate sul dispositivo mobile del passeggero, si limitano a conservare esclusivamente i dati del documento di riconoscimento utilizzato ai fini dell'enrollment e l'immagine/selfie dello stesso.

Ne consegue che le DTC non consentono, a differenza di quanto sostenuto dalla Società, di assicurare un controllo attivo, da parte dell'interessato, sui propri dati biometrici, che rimangono invece nell'esclusiva disponibilità del gestore aeroportuale.

Rispetto alle modalità di conservazione dei modelli biometrici, è emerso, altresì, che SEA non ha adottato misure di cifratura degli stessi, all'atto della relativa conservazione nei propri sistemi; ciò ritenendo sufficienti, in termini di adeguatezza ai sensi dell'art. 32 del Regolamento, le misure complessivamente implementate dalla stessa.

Si fa riferimento, in particolare, a quella inerente alla segregazione fisica dei dati in data-base distinti, a quella inerente alla cifratura selettiva delle sole banche dati contenenti le informazioni riportate nelle DTC e nelle carte d'imbarco, nonché a quella riguardante l'adozione di controlli di accesso indipendenti (v. par. 3.3, lett. b) del presente provvedimento).

Sul punto, si rileva di contro che la natura particolarmente delicata dei dati oggetto di conservazione da parte di SEA rende ad ogni modo necessaria l'applicazione di sistemi di cifratura dei modelli biometrici, ancorché gli stessi siano conservati in un database separato dagli altri dati identificativi dell'interessato. Tale circostanza trova conferma anche nell'Opinion 11/2024 (v. paragrafi 69-71).

È lo stesso Comitato, infatti, a ritenere, proprio con riferimento allo Scenario 3.1., che la misura della compartimentazione dei dati del passeggero in tre banche dati distinte non è di per sé idonea a garantire un livello di sicurezza adeguato a quanto richiesto dall'art. 32 del Regolamento; ciò in ragione "dell'elevata quantità e qualità dei dati di identificazione e dei dati biometrici in possesso del titolare del trattamento", del possibile maggiore impatto che un data breach potrebbe comportare "a causa della conservazione dei dati in un luogo centralizzato", nonché della probabilità di esposizione di "un gran numero di interessati a rischi elevati in termini di gravità, ad esempio il furto d'identità su larga scala" (v. EDPB, Opinion 11/2024, par. 70).

Si aggiunga altresì che, con specifico riferimento ai trattamenti effettuati in caso di adesione del passeggero al "Programma a lungo termine" è stata constatata la conservazione dei template biometrici per un periodo fino a 12 mesi.

La previsione di un termine di conservazione così lungo, rispetto a dati di natura biometrica, comporta come peraltro osservato anche dall'EDPB (Opinion 11/2024, parr. 69, 70 e 73) un

aumento significativo dei rischi associati alle violazioni dei dati personali degli interessati; rischio che non appare adeguatamente controbilanciato dalle misure di sicurezza adottate allo stato dalla Società, né dalla sopra descritta architettura centralizzata del sistema.

Alla luce di quanto premesso, le menzionate previsioni in materia di conservazione delle informazioni biometriche dei passeggeri risultano in contrasto con gli artt. 5, par. 1 lett. e) e 32 del Regolamento.

Sotto altro profilo, con riguardo alla conformità del trattamento in questione al principio di trasparenza, si osserva che il modello di informativa rilasciata da SEA agli interessati, ai sensi dell'art. 13 del Regolamento, conteneva, come accertato nel corso dell'attività ispettiva, alcune indicazioni inesatte in ordine alla conservazione del modello biometrico del passeggero aderente al sistema per il tramite l'App dedicata.

La predetta informativa, infatti, riportava erroneamente che tale modello fosse conservato esclusivamente nel dispositivo mobile dell'interessato, diversamente da quanto è stato invece verificato in sede di ispezione. Il tutto in violazione dell'art. 13 del Regolamento.

Da ultimo, è emerso che la Società ha effettuato un trattamento non conforme all'art. 6 del Regolamento con riguardo ai dati dei passeggeri che, pur non avendo aderito al FaceBoarding, hanno utilizzato, all'ingresso dell'area sterile, i varchi ibridi a ciò dedicati.

In tale circostanza, è stato infatti accertato che, al momento del passaggio, viene comunque acquisita dal sistema l'immagine del volto del passeggero e che viene generato seppur per un limitato arco di tempo il template dello stesso; ciò sebbene quest'ultimo non abbia mai rilasciato il consenso al relativo trattamento (ed in assenza di altra idonea base giuridica ai sensi degli artt. 6 e 9 del Regolamento).

Sul punto, non appaiono rilevanti le argomentazioni sostenute dalla Società in ordine alla circostanza che la natura "ibrida" dei predetti varchi fosse adeguatamente segnalata con idonea cartellonistica e che il template biometrico generato venisse cancellato automaticamente in un lasso temporale inferiore a 1,5 secondi dal rilevamento (v. par. 3.3, lett. c) della presente decisione).

I dati biometrici dei passeggeri, infatti, sono stati ad ogni modo trattati seppure per un brevissimo periodo di tempo in assenza di idonea base giuridica.

Per tutte le ragioni complessivamente sopra esposte, la condotta tenuta da SEA è stata posta in contrasto con l'art. 5, paragrafo 1, lett. a) e con l'art. 6 del Regolamento.

Infine rispetto a quanto rilevato da SEA in ordine alla circostanza che l'Autorità era già stata informata nel 2019 dell'avvio di un sistema di riconoscimento facciale dei passeggeri presso l'aeroporto di Milano Linate e che, in ordine allo stesso, era stato anche effettuato un accertamento ispettivo nelle date del 5 e del 6 giugno 2023, senza che allo stesso avesse fatto seguito una contestazione ai sensi dell'art. 166, comma 5 del Codice (v. par. 3.3., lett. a) del presente provvedimento) occorre precisare che tale specifica istruttoria ha riguardato un sistema di riconoscimento facciale diverso da quello oggetto del presente provvedimento.

Il precedente sistema, infatti, si basava innanzi tutto su un'architettura tecnica e strutturale non coincidente con quella dell'attuale FaceBoarding ed era stato, peraltro, sviluppato da un differente fornitore.

Inoltre, lo stesso era stato avviato dalla Società in via prettamente sperimentale, in quanto contemplato nell'ambito di un progetto pilota di portata circoscritta (riguardava, infatti, solo alcune tratte aeree specificatamente individuate) e limitato nel tempo.

Tale progetto è inoltre terminato il 19 febbraio 2024, ovvero in data antecedente all'adozione, da parte dell'EDPB, dell'Opinion 11/2024.

5. Conclusioni: dichiarazione di illiceità del trattamento.

Alla luce di quanto rilevato, l'Autorità ritiene che le dichiarazioni, la documentazione e le ricostruzioni fornite dal titolare del trattamento nel corso dell'istruttoria, non consentano di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e che non siano pertanto idonei a disporre l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali effettuato da SEA risulta infatti illecito, nei termini su esposti, con riferimento alla violazione dell'art. 5, paragrafo 1, lettere a) e) e f), e agli articoli 6, 13, 25 e 32 Regolamento.

La predetta condotta è stata posta in essere per circa un anno (nello specifico dal 7 maggio 2024 al 16 settembre 2025) e ha coinvolto 24.550 interessati.

Preso atto della circostanza che la Società, il 16 settembre 2025, ha provveduto ad interrompere ogni attività di trattamento per il tramite del sistema FaceBoarding, nonché a cancellare dai propri sistemi i dati personali dei passeggeri oggetto delle predette attività, si ritiene che non ricorrano, allo stato degli atti, i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2 del Regolamento.

[OMISSIS]

TUTTO CIÒ PREMESSO, IL GARANTE

a) dichiara, ai sensi degli artt. 57, par. 1, lett. a) del Regolamento, l'illiceità del trattamento effettuato da Società per Azioni Esercizi Aeroportuali S.E.A., con sede in Segrate (MI), p. iva n. 00826040156, nei termini di cui in premessa, per la violazione dell'art. 5, paragrafo 1, lettere a) e) e f), e degli articoli 6, 13, 25 e 32 Regolamento;

b) *[OMISSIS]*

c) prevede, ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento;

d) dispone, ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità.

Ai sensi dell'art. 78 del Regolamento (UE) 2016/679, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 12 marzo 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL VICE SEGRETARIO GENERALE
Filippi