



Consiglio
dell'Unione europea

Bruxelles, 14 dicembre 2022
(OR. en)

15719/22

**Fascicolo interistituzionale:
2022/0425(COD)**

**IXIM 292
ENFOPOL 639
AVIATION 319
DATAPROTECT 363
JAI 1678
CODEC 2012
IA 223**

PROPOSTA

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	14 dicembre 2022
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2022) 731 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sulla raccolta e sul trasferimento di informazioni anticipate sui passeggeri a fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi, e che modifica il regolamento (UE) 2019/818

Si trasmette in allegato, per le delegazioni, il documento COM(2022) 731 final.

All.: COM(2022) 731 final



COMMISSIONE
EUROPEA

Strasburgo, 13.12.2022
COM(2022) 731 final

2022/0425 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sulla raccolta e sul trasferimento di informazioni anticipate sui passeggeri a fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi, e che modifica il regolamento (UE) 2019/818

{SWD(2022) 424 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• **Motivi e obiettivi della proposta**

Nel corso dell'ultimo decennio, nell'UE e in altre parti del mondo è stato rilevato un aumento dei reati gravi e di criminalità organizzata. Secondo la valutazione di Europol della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità dell'UE, la maggior parte dei fenomeni di criminalità organizzata implica viaggi internazionali, solitamente finalizzati al traffico di persone, stupefacenti o altre merci illecite nell'UE. In particolare, i criminali ricorrono spesso ai principali aeroporti dell'UE come pure ad aeroporti regionali più piccoli in cui operano compagnie aeree low-cost¹. Analogamente, la relazione di Europol sulla situazione e sulle tendenze del terrorismo mostra che la minaccia terroristica nell'UE rimane concreta e grave², facendo notare che la maggior parte delle azioni terroristiche sono di carattere transnazionale e implicano contatti transnazionali o viaggi all'esterno dell'UE. In tale contesto, le informazioni sui viaggiatori aerei costituiscono per le autorità di contrasto uno strumento importante per combattere il terrorismo e i reati gravi nell'UE.

I dati sui viaggiatori aerei comprendono le informazioni anticipate sui passeggeri (API) e i dati del codice di prenotazione (PNR) che, se utilizzati insieme, sono particolarmente efficaci per individuare i viaggiatori ad alto rischio e confermare il modello di viaggio delle persone sospette. Quando un passeggero acquista un biglietto presso un vettore aereo, il sistema di prenotazione di quest'ultimo genera per finalità commerciali un PNR, che comprende i dati sull'intero itinerario, i dati di pagamento, i dati di contatto e le richieste particolari del passeggero. Qualora si applichi un obbligo in tal senso, i dati PNR sono inviati all'unità d'informazione sui passeggeri (UIP) del paese di destinazione e spesso a quella del paese di partenza.

Nell'UE, la direttiva PNR³ adottata nel 2016 garantisce che tutti gli Stati membri attuino norme sulla raccolta dei dati PNR dei vettori aerei per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi, fatte salve le norme europee sull'obbligo per i vettori aerei di raccogliere i dati API previste dalla direttiva API⁴. Nel quadro della direttiva PNR, gli Stati membri devono adottare i provvedimenti necessari affinché i vettori aerei trasferiscano i dati PNR a condizione che abbiano già raccolto tali dati nel normale svolgimento della loro attività. La direttiva PNR prevede il trattamento congiunto sia dei dati API che dei dati PNR, in quanto la definizione di dati PNR comprende le "informazioni anticipate sui passeggeri (API) eventualmente raccolte"⁵. Tuttavia, la direttiva PNR non impone ai vettori aerei l'obbligo di raccogliere altri dati oltre a quelli necessari per il normale

¹ Europol, "Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità dell'UE" (SOCTA), 2021,

https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

² Europol, "Relazione sulla situazione e sulle tendenze del terrorismo" (Te-SAT), 2021,

https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf.

³ Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

⁴ Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

⁵ Cfr. allegato I, punto 18, della direttiva (UE) 2016/681.

svolgimento della loro attività. Di conseguenza, la direttiva PNR non prevede la raccolta dell'intera serie di dati API, in quanto i vettori aerei non hanno alcuna finalità commerciale per raccogliere tali dati.

Solo laddove si applichi un obbligo in tal senso, il vettore aereo raccoglie durante il check-in del passeggero (check-in online e in aeroporto) i dati API, che sono quindi inviati alle autorità di frontiera competenti sotto forma di un "manifesto dell'elenco di passeggeri" completo che riporta tutti i passeggeri imbarcati alla partenza dell'aereo. Mentre i dati API sono considerati informazioni "verificate" in quanto corrispondono ai viaggiatori che si sono effettivamente imbarcati sul velivolo, e possono essere utilizzati anche dalle autorità di contrasto per individuare persone sospette e ricercati, i dati PNR sono informazioni "non verificate" fornite dai passeggeri. I dati PNR di un determinato passeggero non contengono solitamente tutti i possibili elementi PNR ma solo quelli forniti dal passeggero e/o necessari per la prenotazione e, quindi, per le normali finalità commerciali del vettore aereo.

Dall'adozione della direttiva API nel 2004 sussiste un consenso globale riguardo al fatto che i dati API costituiscono non solo uno strumento chiave per la gestione delle frontiere ma anche uno strumento importante per le finalità di contrasto, segnatamente per contrastare il terrorismo e i reati gravi. A livello internazionale, dal 2014, le risoluzioni del Consiglio di sicurezza delle Nazioni Unite hanno pertanto più volte esortato a creare e introdurre a livello globale sistemi PNR e API per fini di contrasto⁶. Inoltre, l'impegno da parte degli Stati che partecipano all'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) di istituire sistemi API conferma l'importanza dell'utilizzo di tali dati nella lotta contro il terrorismo e i reati transnazionali.⁷

Come illustrato dalla relazione della Commissione sul riesame della direttiva PNR, il trattamento congiunto dei dati PNR e API da parte delle autorità di contrasto competenti (per cui i dati PNR raccolti dai vettori aerei per le loro normali finalità commerciali e trasferiti alle autorità di contrasto competenti sono integrati da un obbligo per i vettori aerei di raccogliere e trasferire i dati API) aumenta in modo sostanziale l'efficacia della lotta contro il terrorismo e i reati gravi nell'UE⁸. L'utilizzo congiunto dei dati API e dei dati PNR consente alle autorità nazionali competenti di confermare l'identità dei passeggeri e di migliorare in modo significativo l'affidabilità dei dati PNR. Tale utilizzo congiunto prima dell'arrivo consente inoltre alle autorità di contrasto di sottoporre a una valutazione e a un controllo più approfondito solo le persone che con maggiore probabilità, secondo pratiche e criteri di valutazione oggettivi e conformemente alla normativa applicabile, costituiscono una minaccia per la sicurezza. Ciò agevola il viaggio di tutti gli altri passeggeri e riduce il rischio che i passeggeri siano sottoposti ad accertamenti all'arrivo da parte delle autorità competenti sulla base di elementi discrezionali quali la razza o l'origine etnica, che possono essere erroneamente associati a rischi di sicurezza dalle autorità di contrasto.

Tuttavia, il quadro giuridico europeo vigente disciplina solo l'utilizzo dei dati PNR per il contrasto del terrorismo e di reati gravi ma non prevede specificamente l'uso dei dati API, che

⁶ Si vedano le risoluzioni del Consiglio di sicurezza delle Nazioni Unite 2178(2014), 2309(2016), 2396(2017), 2482(2019) come pure la [decisione del Consiglio dei ministri 6/16](#) dell'OSCE del 9 dicembre 2016 sul rafforzamento dell'uso delle informazioni anticipate sui passeggeri.

⁷ [Decisione del Consiglio dei ministri 6/16](#) dell'OSCE, del 9 dicembre 2016 sul rafforzamento dell'uso delle informazioni anticipate sui passeggeri.

⁸ Commissione europea, documento di lavoro dei servizi della Commissione che accompagna la relazione sul riesame della direttiva 2016/681 (SWD(2020) 128 final).

può essere richiesto solo per i voli provenienti dai paesi terzi: ciò produce una lacuna a livello di sicurezza, segnatamente per quanto riguarda i voli intra-UE per i quali gli Stati membri chiedono ai vettori aerei di trasferire i dati PNR. Le unità d'informazione sui passeggeri ottengono i risultati operativi più efficaci sui voli in cui sono raccolti i dati sia PNR che API. Ciò significa che le autorità di contrasto competenti non possono beneficiare dei risultati del trattamento congiunto dei dati API e dei dati PNR sui voli all'interno dell'UE, per i quali sono trasferiti solo i dati PNR.

Per ovviare a tale lacuna, il documento di giugno 2021 della Commissione intitolato "Strategia per uno spazio Schengen senza controlli alle frontiere interne pienamente funzionante e resiliente" ha invitato ad accrescere l'uso dei dati API in combinazione con i dati PNR per i voli intra-Schengen così da migliorare notevolmente la sicurezza interna, in conformità con i diritti fondamentale alla protezione dei dati personali e alla libertà di circolazione⁹.

La proposta di regolamento mira pertanto a definire norme migliori per la raccolta e il trasferimento di dati API da parte dei vettori aerei per fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi. Al fine di garantire la conformità con i diritti fondamentali pertinenti sanciti nella Carta dei diritti fondamentali dell'UE ("Carta"), in particolare i diritti alla vita privata e alla protezione dei dati personali, e i conseguenti obblighi in materia di necessità e proporzionalità, la proposta contiene, come ulteriormente illustrato in appresso, attente limitazioni per quanto riguarda la portata e misure di salvaguardia e limiti rigorosi sulla protezione dei dati personali.

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

Le norme proposte sulla raccolta e sul trasferimento dei dati API per fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi sono in linea con le norme applicabili per il trattamento dei dati PNR, secondo quanto stabilito nella direttiva PNR¹⁰. Tengono conto delle interpretazioni della Corte di giustizia dell'Unione europea nella sua recente giurisprudenza, segnatamente ciò che quest'ultima specifica riguardo al trattamento dei dati PNR per i voli intra-UE, per cui il trasferimento dei dati PNR alle autorità competenti degli Stati membri sui voli intra-UE deve essere selettivo e non può essere sistematico se non giustificato da una minaccia terroristica reale e attuale o prevedibile¹¹.

Nella misura in cui sussiste una possibile sovrapposizione tra la proposta di regolamento e le norme di cui alla direttiva PNR, dal momento che (come menzionato) nel quadro di tale direttiva la definizione di "dati PNR" comprende le "informazioni anticipate sui passeggeri (API) eventualmente raccolte", prevalgono le norme di cui al regolamento proposto, poiché si tratta sia di *lex specialis* che *lex posterior*. Mentre nel quadro della direttiva PNR gli Stati membri devono adottare i necessari provvedimenti affinché i vettori aerei trasferiscano i dati PNR a condizione che abbiano già raccolto tali dati nel normale svolgimento della loro attività, il regolamento proposto fa obbligo ai vettori aerei di raccogliere i dati API in situazioni specifiche e di trasferire tali dati in un modo specifico. La proposta di regolamento

⁹ COM(2021) 277 final (2.6.2021).

¹⁰ La direttiva PNR fissa le condizioni per il trattamento dei dati, ad esempio le autorità competenti (articolo 7), il periodo di conservazione dei dati (articolo 12) e la protezione dei dati personali (articolo 13).

¹¹ Sentenza della Corte di giustizia nella causa C-817/19, *Ligue des droits humains*.

integra pertanto la direttiva PNR, in quanto garantisce che, in tutti i casi in cui le autorità di contrasto competenti (vale a dire le unità d'informazione sui passeggeri) ricevono i dati PNR in virtù della direttiva PNR, i vettori aerei sono tenuti a raccogliere e trasferire i dati API a tali autorità competenti.

A seguito della trasmissione dei dati API alle unità d'informazione sui passeggeri (UIP) istituite dalla direttiva PNR, oltre alle limitate prescrizioni a tale proposito previste dalla proposta di regolamento, si applicano le norme sul successivo trattamento dei dati API da parte delle UIP che figurano nella direttiva PNR. Come menzionato, la direttiva PNR prevede il trattamento congiunto dei dati API e dei dati PNR, in quanto la definizione di dati PNR comprende le "informazioni anticipate sui passeggeri (API) eventualmente raccolte", e pertanto i dati API ricevuti dalle UIP secondo il regolamento proposto. Di conseguenza si applicano le norme di cui all'articolo 6 e all'articolo 9 e seguenti della direttiva PNR in relazione a questioni quali le finalità esatte del trattamento, i periodi di conservazione, la cancellazione, lo scambio di informazioni, il trasferimento dagli Stati membri a paesi terzi e le disposizioni specifiche sulla protezione di tali dati personali.

Si applicheranno inoltre gli atti del diritto dell'UE solitamente applicabili in conformità con le condizioni da essi previste. Per quanto riguarda il trattamento dei dati personali, si tratta in particolare del regolamento generale sulla protezione dei dati¹², della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie¹³ e del regolamento sulla protezione dei dati nelle istituzioni dell'UE¹⁴. Tali atti non sono alterati dalla presente proposta.

L'applicabilità degli atti citati del diritto dell'UE al trattamento dei dati API ricevuti a norma del presente regolamento comporta il fatto che gli Stati membri attuano il diritto dell'UE ai sensi dell'articolo 51, paragrafo 1, della Carta; pertanto si applicano anche le norme della Carta. In particolare, le norme di tali atti del diritto dell'UE devono essere interpretate alla luce della Carta.

Garantendo la coerenza con le norme di cui alla proposta di regolamento sulla raccolta e sul trasferimento dei dati API a fini di controllo di frontiera e di efficienza nelle trasmissioni dei dati API, la presente proposta prevede l'obbligo per i vettori aerei di raccogliere la medesima serie di dati API e di trasferirla al medesimo router creato in virtù dell'altra proposta di regolamento.

La raccolta dei dati API dai documenti di viaggio è inoltre coerente con le linee guida dell'ICAO sui documenti di viaggio a lettura ottica¹⁵, che sono state recepite nel regolamento (UE) 2019/1157 sul rafforzamento della sicurezza delle carte d'identità dei cittadini

¹² 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.

¹³ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

¹⁴ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

¹⁵ ICAO, documento 9303, "Machine Readable Travel Documents", ottava edizione, 2021, disponibile all'indirizzo: https://www.icao.int/publications/documents/9303_p1_cons_en.pdf.

dell'Unione, nella direttiva (UE) 2019/997 del Consiglio sui documenti di viaggio provvisori dell'UE e nel regolamento (CE) n. 2252/2004 relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti. Tali regolamenti permettono di estrarre dati completi e di qualità elevata dai documenti di viaggio in maniera automatizzata.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

• Base giuridica

Per la presente proposta di regolamento sulla raccolta e sul trasferimento dei dati API per attività di prevenzione, accertamento, indagine e perseguimento riguardo ai reati di terrorismo e ai reati gravi, in considerazione del suo obiettivo e delle misure previste, la base giuridica idonea è costituita dall'articolo 82, paragrafo 1, lettera d), e dall'articolo 87, paragrafo 2, lettera a), del trattato sul funzionamento dell'Unione europea (TFUE).

In virtù dell'articolo 82, paragrafo 1, lettera d), TFUE, l'Unione ha la facoltà di adottare misure intese a facilitare la cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni. A norma dell'articolo 87, paragrafo 2, lettera a), TFUE, l'Unione ha la facoltà di adottare misure riguardanti la raccolta, la conservazione, il trattamento, l'analisi e lo scambio di informazioni pertinenti per fini di cooperazione di polizia nell'UE.

Di conseguenza, la base giuridica utilizzata per la presente proposta è la medesima utilizzata per la direttiva PNR, che è adeguata in considerazione non solo del fatto che la proposta di regolamento persegue fundamentalmente il medesimo obiettivo, ma anche che integra la direttiva PNR.

• Sussidiarietà

Alle autorità di contrasto devono essere forniti strumenti efficaci per la lotta contro i reati di terrorismo e altri reati gravi. Siccome la maggior parte dei reati gravi e degli atti terroristici comporta viaggi internazionali, spesso attraverso i trasporti aerei, i dati PNR si sono dimostrati molto efficienti nella protezione della sicurezza interna dell'UE. Inoltre, le indagini per fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi svolte dalle autorità competenti degli Stati membri si basano in gran parte sulla cooperazione transfrontaliera e internazionale.

In uno spazio senza controlli alle frontiere interne, la raccolta, il trattamento e lo scambio di dati dei passeggeri, ivi compresi i dati API e PNR, da parte degli Stati membri costituiscono anche misure di compensazione efficienti. Prevedendo un'azione coerente a livello dell'UE, la proposta contribuirà ad aumentare la sicurezza degli Stati membri e, di conseguenza, dell'UE nel suo insieme.

La direttiva API fa parte dell'*acquis* di Schengen relativo all'attraversamento delle frontiere esterne. Non disciplina pertanto la raccolta e il trasferimento dei dati API sui voli intra-UE. In assenza di dati API per l'integrazione dei dati PNR relativi a tali voli, gli Stati membri hanno attuato varie misure volte a compensare la mancanza di dati di identità sui passeggeri. Tra tali misure figurano i controlli di conformità fisici effettuati per verificare se i dati di identità indicati nel documento di viaggio corrispondono a quelli della carta di imbarco, che generano nuovi problemi senza risolvere il problema di fondo della mancanza di dati API.

L'azione a livello dell'UE contribuirà a garantire l'applicazione di disposizioni armonizzate sulla salvaguardia dei diritti fondamentali, in particolare la protezione dei dati personali, negli Stati membri. I vari sistemi degli Stati membri che hanno già creato o creeranno meccanismi analoghi potrebbero avere effetti negativi sui vettori aerei in quanto potrebbero dover seguire

prescrizioni nazionali divergenti, ad esempio riguardo al tipo di informazioni da trasferire e alle condizioni alle quali tali informazioni devono essere fornite agli Stati membri. Tali differenze compromettono la cooperazione efficace tra gli Stati membri a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Tali norme armonizzate possono essere definite solo a livello dell'UE.

Poiché gli obiettivi della presente proposta non possono essere conseguiti adeguatamente dagli Stati membri e possono essere conseguiti meglio a livello dell'Unione, si può concludere che l'UE è nel contempo autorizzata ad intervenire e in una posizione migliore per farlo rispetto ai singoli Stati membri. La proposta rispetta pertanto il principio di sussidiarietà enunciato all'articolo 5 del trattato sull'Unione europea.

- **Proporzionalità**

Secondo il principio di proporzionalità di cui all'articolo 5, paragrafo 4, TUE, la natura e l'intensità di una misura devono corrispondere a quelle del problema individuato. Tutti i problemi affrontati dalla presente iniziativa legislativa richiedono in un modo o nell'altro un intervento legislativo a livello dell'UE che consenta agli Stati membri di affrontarli efficacemente.

Le norme proposte sulla raccolta e sul trasferimento dei dati API, nel rispetto di misure di salvaguardia e limitazioni rigorose, rafforzeranno la prevenzione, l'accertamento, l'indagine e l'azione penale nei confronti dei reati di terrorismo e dei reati gravi. Le norme proposte corrispondono pertanto all'esigenza individuata di rafforzare la sicurezza interna, rispondendo in modo efficace al problema derivante dall'assenza di un trattamento congiunto dei dati API e dei dati PNR, anche per i voli intra-UE per i quali gli Stati membri ricevono i dati PNR.

L'ambito di applicazione della proposta è limitato a quanto è strettamente necessario, cioè limitato a quegli elementi che richiedono un approccio armonizzato a livello dell'UE, segnatamente le finalità per le quali i dati API possono essere utilizzati dalle unità d'informazione sui passeggeri, gli elementi di dati che devono essere raccolti e i mezzi per la raccolta e il trasferimento dei dati API dei viaggiatori. Il trasferimento dei dati API al router rende meno complesso per i vettori aerei mantenere i collegamenti con le unità d'informazione sui passeggeri e introduce economie di scala, riducendo al contempo la possibilità di errori e usi scorretti. La finalità riguarda solo i reati di terrorismo e i reati gravi, quali definiti nella proposta, alla luce della loro gravità e della loro dimensione transnazionale.

Per limitare l'ingerenza nei diritti dei passeggeri a quanto è strettamente necessario, la proposta comprende una serie di misure di salvaguardia. Più precisamente, il trattamento dei dati API a norma della proposta di regolamento si limita a un elenco esaustivo e limitato di dati API, al di là del quale non devono essere raccolti altri dati di identità. La proposta di regolamento prevede inoltre solo norme sulla raccolta e sul trasferimento di dati API attraverso il router alle UIP per le finalità limitate ivi specificate e non disciplina l'ulteriore trattamento dei dati API da parte delle UIP, in quanto, come sopra illustrato, ciò è disciplinato da altri atti giuridici dell'UE (direttiva PNR, normativa sulla protezione dei dati personali, Carta). Le funzionalità del router e in particolare la sua capacità di raccogliere e fornire informazioni statistiche globali favoriscono anch'esse il monitoraggio dell'attuazione del presente regolamento da parte dei vettori aerei e delle unità d'informazione sui passeggeri. Sono altresì previste determinate misure di salvaguardia specifiche, ad esempio norme in materia di registrazione, protezione dei dati personali e sicurezza.

Per garantire la necessità e la proporzionalità del trasferimento dei dati a norma della proposta di regolamento e, più precisamente, riguardo alla raccolta e al trasferimento dei dati sui voli

intra-UE, gli Stati membri riceveranno solo i dati API per i voli intra-UE che hanno selezionato in linea con la giurisprudenza sopraccitata della Corte di giustizia. Inoltre, l'ulteriore trattamento dei dati API da parte delle UIP sarebbe soggetto ai limiti e alle misure di salvaguardia di cui alla direttiva PNR, come interpretata dalla Corte di giustizia nella causa *Ligue des droits humains*¹⁶ alla luce della Carta.

- **Scelta dell'atto giuridico**

La misura proposta è un regolamento. Alla luce della necessità che le misure proposte siano direttamente applicabili e applicate in modo uniforme in tutti gli Stati membri, un regolamento costituisce l'atto giuridico opportuno.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- **Valutazione ex post della legislazione vigente**

La direttiva API non impedisce il trattamento dei dati API per fini di contrasto come stabilito nella legislazione nazionale e nel rispetto delle prescrizioni sulla protezione dei dati personali. L'attuazione di tale possibilità in tutti gli Stati membri è tuttavia problematica, come rilevato nella valutazione della direttiva API, con conseguenti lacune in materia di sicurezza causate da una mancanza di criteri definiti a livello dell'UE sulla raccolta e sul trasferimento dei dati API per fini di contrasto¹⁷:

- la finalità di contrasto è interpretata in senso ampio negli ordinamenti nazionali di alcuni Stati membri: dai reati amministrativi, al rafforzamento dell'ordine pubblico e della sicurezza interna, alla lotta contro il terrorismo, alla salvaguardia degli interessi di sicurezza nazionali. La valutazione della direttiva API indica altresì che un utilizzo efficace dei dati API per fini di contrasto richiederebbe uno strumento giuridico apposito per tale finalità specifica¹⁸;
- la varietà dei fini per cui sono raccolti i dati API rende ancora più difficile garantire la conformità con il quadro dell'UE sulla protezione dei dati personali. L'obbligo di cancellazione dei dati API entro 24 ore si applica solo se i dati API sono usati per l'obiettivo principale della direttiva API, ossia la gestione delle frontiere esterne. Non è chiaro se tale obbligo si applichi anche in relazione al trattamento svolto per fini di contrasto;
- la serie di dati API che può essere richiesta dai vettori per finalità di contrasto, insieme alla prassi di alcuni Stati membri di richiedere dati API non compresi nell'elenco non esaustivo previsto dalla direttiva API, rendono ancora più difficile per i vettori aerei rispettare i diversi requisiti durante il trasporto di passeggeri verso l'UE;
- analogamente, la direttiva API non fornisce alcuna indicazione riguardo ai voli per i quali possono essere richiesti i dati API, alle autorità a cui i dati API devono essere trasferiti o alle condizioni di accesso a tali dati per fini di contrasto.

¹⁶ Sentenza della Corte di giustizia del 21 giugno 2022, C-817/19, *Ligue des droits humains*.

¹⁷ Documento di lavoro dei servizi della Commissione europea, dell'8 settembre 2020, dal titolo "Valutazione della direttiva 2004/82/CE del Consiglio concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate (direttiva API)" (SWD(2020) 174 final), Bruxelles, pagg. 26 e 43.

¹⁸ SWD(2020) 174, pag. 57.

- **Consultazioni dei portatori di interessi**

L'elaborazione della presente proposta ha comportato un'ampia serie di consultazioni dei portatori di interessi, ivi compresi le autorità degli Stati membri (autorità di frontiera competenti, unità d'informazione sui passeggeri), i rappresentanti del settore dei trasporti e singoli vettori. Hanno contribuito anche le agenzie dell'UE, quali l'Agenzia europea della guardia di frontiera e costiera (Frontex), l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) e l'Agenzia dell'Unione europea per i diritti fondamentali (FRA). La presente iniziativa integra inoltre i pareri e le osservazioni ricevuti durante la consultazione pubblica svolta alla fine del 2019 nel quadro della valutazione della direttiva API¹⁹.

Le attività di consultazione nel contesto della preparazione della valutazione d'impatto su cui si basa la presente proposta hanno consentito di raccogliere le osservazioni dei portatori di interessi con vari metodi. Sono stati svolti, in particolare, una valutazione d'impatto iniziale, uno studio di sostegno esterno e una serie di seminari tecnici.

Dal 5 giugno 2020 al 14 agosto 2020 è stata pubblicata una valutazione d'impatto iniziale al fine di raccogliere osservazioni: i sette contributi ricevuti hanno fornito osservazioni riguardanti l'ambito di applicazione della futura direttiva API, la qualità dei dati, le sanzioni, il rapporto tra i dati API e i dati PNR, la protezione dei dati personali²⁰.

Lo studio di sostegno esterno è stato svolto sulla base di ricerche documentali, interviste e sondaggi con esperti in materia che hanno esaminato varie misure possibili per trattare i dati API secondo norme chiare che agevolino i viaggi legittimi e siano compatibili con l'interoperabilità dei sistemi di informazione dell'UE, gli obblighi in materia di protezione dei dati personali dell'UE, altri strumenti dell'UE vigenti e norme internazionali.

I servizi della Commissione hanno organizzato una serie di seminari tecnici con esperti degli Stati membri e dei paesi associati Schengen, che hanno scambiato opinioni sulle possibili opzioni previste per rafforzare il futuro quadro API a fini di gestione delle frontiere e lotta contro la criminalità e il terrorismo.

La valutazione d'impatto che accompagna la presente proposta riporta una descrizione più dettagliata della consultazione dei portatori di interessi (allegato 2).

- **Valutazione d'impatto**

Conformemente alle linee guida per legiferare meglio, la Commissione ha effettuato una valutazione d'impatto, presentata nel documento dei servizi che accompagna la presente proposta [riferimento]. Il comitato per il controllo normativo ha riesaminato il progetto di valutazione d'impatto nella riunione del 28 settembre 2022 e ha espresso un parere positivo il 30 settembre 2022.

Alla luce dei problemi individuati sulla raccolta e sul trasferimento dei dati API, nella valutazione d'impatto sono state valutate le opzioni strategiche sulla portata della raccolta dei dati API per la gestione delle frontiere esterne e per fini di contrasto, unitamente alle opzioni sui mezzi per migliorare la qualità dei dati API. Riguardo alla raccolta dei dati API per fini di contrasto, la valutazione d'impatto ha preso in considerazione, da un lato, la raccolta dei dati

¹⁹ SWD(2020) 174.

²⁰ <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12434-Controlli-alle-frontiere-e-attivita-di-contrasto-norme-rivedute-sulle-informazioni-anticipate-sui-passeggeri-del-trasporto-aereo-API-it>.

API di tutti i voli extra-UE, dall'altro la raccolta dei dati API di tutti i voli extra-UE e di voli intra-UE selezionati. Inoltre, la valutazione d'impatto ha tenuto conto delle possibilità di miglioramento della qualità dei dati API: raccogliere i dati API con mezzi sia automatizzati che manuali, oppure soltanto con mezzi automatizzati.

In base ai risultati della relazione sulla valutazione d'impatto, l'opzione prescelta per uno strumento API per fini di contrasto comprende la raccolta dei dati API di tutti i voli all'interno e all'esterno dell'UE, e dei voli intra-UE selezionati per i quali sono trasferiti i dati PNR. Ciò rafforzerà in modo significativo la validità dell'analisi dei dati pertinenti riguardanti i viaggiatori aerei necessaria per la lotta contro i reati gravi e il terrorismo, in quanto le unità d'informazione sui passeggeri avranno a disposizione i dati API, verificati e pertanto di migliore qualità, al fine di individuare le persone coinvolte in reati gravi o di terrorismo. La raccolta e il trasferimento dei dati API per fini di contrasto si baseranno sulle capacità sviluppate per il trasferimento dei dati API, attraverso il router, per la gestione delle frontiere esterne, senza alcun costo aggiuntivo per eu-LISA. I vettori aerei trasferiranno i dati API solo al router, che li trasferirà a sua volta all'unità d'informazione sui passeggeri di ciascuno Stato membro interessato. La valutazione d'impatto ha concluso che ciò costituisce una soluzione efficiente sotto il profilo dei costi per i vettori aerei, in quanto riduce i costi di trasmissione sostenuti dai vettori aerei, limitando al contempo la possibilità di errori o usi scorretti. Tuttavia, diversamente dalla situazione attuale, la proposta di regolamento prevede che i vettori aerei raccolgano e trasferiscano i dati API di tutti i voli contemplati dalla presente proposta, indipendentemente dalle loro normali esigenze commerciali e compresi i voli intra-UE. La proposta è in linea con l'obiettivo di neutralità climatica di cui alla normativa europea sul clima²¹ nonché con gli obiettivi dell'Unione per il 2030 e il 2040.

- **Diritti fondamentali**

La presente iniziativa prevede il trattamento dei dati personali dei viaggiatori e limita pertanto l'esercizio del diritto fondamentale alla protezione dei dati personali quale garantito dall'articolo 8 della Carta e dall'articolo 16 TFUE. Come sottolineato dalla Corte di giustizia dell'UE²², il diritto alla protezione dei dati personali non costituisce una prerogativa assoluta ma ogni eventuale limitazione va considerata alla luce della sua funzione sociale e deve rispettare i criteri di cui all'articolo 52, paragrafo 1, della Carta²³. La protezione dei dati personali è altresì strettamente connessa al rispetto del diritto alla vita privata, quale parte del diritto alla vita privata e alla vita familiare sancito dall'articolo 7 della Carta.

Per quanto riguarda la raccolta e il trasferimento dei dati API per i voli intra-UE selezionati, la presente iniziativa influisce altresì sull'esercizio del diritto fondamentale alla libertà di circolazione di cui all'articolo 45 della Carta e all'articolo 21 TFUE. Secondo la Corte di giustizia, la restrizione alla libera circolazione delle persone può essere giustificata solo se è

²¹ Articolo 2, paragrafo 1, del regolamento (UE) 2021/1119, del 30 giugno 2021, che istituisce il quadro per il conseguimento della neutralità climatica ("normativa europea sul clima").

²² Sentenza della Corte di giustizia del 9 novembre 2010, cause riunite C-92/09 e C-93/09 *Volker und Markus Schecke ed Eifert* [2010], ECR I-0000.

²³ Conformemente all'articolo 52, paragrafo 1, della Carta, possono essere apportate limitazioni all'esercizio del diritto alla protezione dei dati purché esse siano previste dalla legge, rispettino il contenuto essenziale del diritto e delle libertà e, in ottemperanza al principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

basata su considerazioni oggettive ed è proporzionata allo scopo legittimamente perseguito dal diritto nazionale²⁴.

In virtù del presente regolamento, la raccolta e il trasferimento dei dati API possono essere effettuati solo per fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e altri reati gravi, quali definiti nella direttiva PNR. Le disposizioni di cui alla presente proposta stabiliscono criteri uniformi per la raccolta e il trasferimento dei dati API, da un lato, dei voli extra-UE (in arrivo e in partenza) e, dall'altro lato, dei voli intra-UE selezionati, sulla base di una valutazione effettuata dagli Stati membri e oggetto di riesame periodico, in linea con gli obblighi stabiliti dalla Corte di giustizia nella causa *Ligue des droits humains*. L'obbligo dei vettori aerei di raccogliere e trasferire i dati API al router riguarda tutti i voli intra-UE. La trasmissione da parte del router alle UIP costituisce una soluzione tecnica per limitare la trasmissione dei dati API alle unità d'informazione sui passeggeri solo ai voli selezionati, senza divulgare informazioni riservate su quali siano i voli intra-UE selezionati. Tali informazioni devono essere trattate in modo riservato, alla luce del rischio di elusione che sussisterebbe se dovessero essere note al pubblico o, più nello specifico, a persone coinvolte in attività terroristiche o reati gravi.

L'utilizzo obbligatorio di mezzi automatizzati da parte dei vettori aerei per raccogliere determinati dati API dei viaggiatori può comportare rischi, anche dal punto di vista della protezione dei dati personali. Tali rischi sono stati tuttavia limitati e mitigati. In primo luogo, la prescrizione si applica solo nei confronti di determinati dati API, laddove i mezzi automatizzati possano essere utilizzati in modo responsabile, vale a dire per i dati leggibili da dispositivo automatico sui documenti dei viaggiatori. In secondo luogo, la proposta di regolamento stabilisce obblighi riguardanti i mezzi automatizzati da utilizzare, che devono essere ulteriormente specificati in un atto delegato. Infine sono previste varie misure di salvaguardia, ad esempio in materia di registrazione, norme specifiche sulla protezione dei dati personali e un controllo efficace.

Inoltre, al di là della disposizione che garantisce l'osservanza del principio di limitazione delle finalità, sebbene la proposta di regolamento non disciplini l'utilizzo che le autorità di frontiera competenti fanno dei dati API che ricevono in virtù della stessa in quanto, come sopra illustrato, ciò è già disciplinato da altre normative, per maggiore chiarezza si ricorda nei considerando che qualsiasi siffatto utilizzo non può portare ad alcuna discriminazione vietata nel quadro dell'articolo 21 della Carta.

4. INCIDENZA SUL BILANCIO

La presente iniziativa legislativa sulla raccolta e sul trasferimento dei dati API, rispettivamente, per agevolare i controlli alle frontiere esterne e per fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi avrebbe ripercussioni sulle esigenze in termini di bilancio e di organico di eu-LISA come pure delle autorità competenti degli Stati membri.

Per quanto riguarda eu-LISA, si calcola che sarebbe necessaria una dotazione aggiuntiva di circa 45 milioni di EUR (33 milioni nel contesto del QFP attuale) per la creazione del router e 9 milioni di EUR all'anno a partire dal 2029 per la relativa gestione tecnica nonché circa 27 posti di lavoro aggiuntivi onde garantire che eu-LISA disponga delle risorse necessarie per svolgere i compiti che le sono assegnati nella presente proposta di regolamento e nella proposta di

²⁴ Sentenza della Corte di giustizia del 5 giugno 2018, causa C-673/16, *Coman*.

regolamento sulla raccolta e sul trasferimento dei dati API per agevolare i controlli alle frontiere esterne.

Si calcola che gli Stati membri possano avere diritto al rimborso da parte del Fondo Sicurezza interna²⁵ di 11 milioni di EUR (3 milioni di EUR nel contesto dell'attuale quadro finanziario pluriennale) dedicati al potenziamento delle infrastrutture e dei sistemi nazionali necessari per le UIP, e a partire dal 2028 di un contributo progressivamente crescente fino a circa 2 milioni di EUR all'anno. Ogni eventuale diritto a beneficiare di tali contributi dovrà in ultima analisi essere determinato in conformità delle norme che disciplinano i fondi in questione nonché delle norme sui costi previste dalla proposta di regolamento.

In considerazione dello stretto legame tra la presente proposta di regolamento e la proposta di regolamento sulla raccolta e sul trasferimento dei dati API per agevolare i controlli alle frontiere esterne, segnatamente riguardo al trasferimento dei dati API al router, la scheda finanziaria legislativa, allegata alla presente proposta di regolamento, è identica per entrambe le proposte.

5. ALTRI ELEMENTI

• Piani attuativi e modalità di monitoraggio, valutazione e informazione

La Commissione assicurerebbe che siano in atto le disposizioni necessarie per monitorare il funzionamento delle misure proposte e valutarle rispetto ai principali obiettivi strategici. Quattro anni dopo l'entrata in vigore della proposta di regolamento API e, successivamente, ogni quattro anni, la Commissione presenterebbe una relazione al Parlamento europeo e al Consiglio concernente la valutazione dell'attuazione del regolamento e del suo valore aggiunto. La relazione segnalerebbe inoltre eventuali impatti diretti o indiretti sui diritti fondamentali. Esaminerebbe i risultati conseguiti rispetto agli obiettivi, valutando nel contempo se i principi di base siano ancora validi e studiando le eventuali implicazioni per le opzioni future.

La natura imperativa dell'obbligo per i vettori aerei di raccogliere i dati API sui voli extra-UE e intra-UE selezionati nonché l'introduzione del router API offrirà una visione più chiara sia sulla trasmissione dei dati API da parte dei vettori aerei che sull'utilizzo dei dati API da parte degli Stati membri in conformità con la legislazione dell'Unione e nazionale applicabile. Ciò sosterrà la Commissione nelle sue attività di contrasto e di valutazione fornendole statistiche affidabili sul volume dei dati trasmessi e sui voli per i quali i dati API sarebbero necessari.

• Illustrazione dettagliata delle singole disposizioni della proposta

Il capo 1 comprende le disposizioni generali del presente regolamento, a cominciare dalle norme sull'oggetto e sull'ambito di applicazione. Contiene altresì un elenco di definizioni.

Il capo 2 comprende le disposizioni per la raccolta, il trasferimento al router e la cancellazione dei dati API da parte dei vettori aerei nonché le norme sulla trasmissione dei dati API dal router alle unità d'informazione sui passeggeri.

Il capo 3 contiene disposizioni specifiche riguardanti le registrazioni nonché precisazioni sui titolari del trattamento dei dati personali in relazione al trattamento dei dati API che costituiscono dati personali in virtù del presente regolamento, sulla sicurezza e sulla verifica interna da parte dei vettori aerei e delle UIP.

²⁵ Regolamento (UE) 2021/1149 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che istituisce il Fondo Sicurezza interna.

Il capo 4 stabilisce norme sui collegamenti al router e sull'integrazione con quest'ultimo da parte delle unità d'informazione sui passeggeri e dei vettori aerei come pure sui relativi costi a carico degli Stati membri. Contiene altresì disposizioni su un'eventuale impossibilità tecnica parziale o completa di utilizzare il router e sulla responsabilità per danni causati al router.

Il capo 5 contiene disposizioni riguardanti il controllo, le possibili sanzioni applicabili ai vettori aerei in caso di mancato adempimento degli obblighi loro imposti dal regolamento e l'elaborazione di un manuale pratico da parte della Commissione.

Il capo 6 contiene modifiche ad altri strumenti esistenti, vale a dire il regolamento (UE) 2019/818.

Il capo 7 contiene le disposizioni finali del regolamento, che riguardano l'adozione di atti delegati, il monitoraggio e la valutazione del regolamento, la sua applicazione ed entrata in vigore.

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sulla raccolta e sul trasferimento di informazioni anticipate sui passeggeri a fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi, e che modifica il regolamento (UE) 2019/818

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 82, paragrafo 1, lettera d), e l'articolo 87, paragrafo 2, lettera a),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo²⁶,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

- (1) La dimensione transnazionale della criminalità organizzata e delle forme gravi di criminalità e la costante minaccia di attacchi terroristici sul territorio europeo impongono di intervenire a livello dell'Unione per adottare misure adeguate che garantiscano la sicurezza in uno spazio di libertà, sicurezza e giustizia senza frontiere interne. Le informazioni sui viaggiatori aerei, come i dati del codice di prenotazione (*Passenger Name Record*, PNR) e in particolare le informazioni anticipate sui passeggeri (*Advance Passenger Information*, API), sono essenziali per identificare i passeggeri ad alto rischio, compresi quelli che non sarebbero altrimenti noti alle autorità di contrasto, e per stabilire collegamenti tra i membri di gruppi criminali e contrastare le attività terroristiche.
- (2) Oltre ad istituire un quadro giuridico per la raccolta e il trasferimento dei dati API da parte dei vettori aerei al fine di migliorare i controlli di frontiera e contrastare l'immigrazione illegale, la direttiva 2004/82/CE del Consiglio²⁷ stabilisce che gli Stati membri possono utilizzare i dati API a fini di contrasto. La semplice creazione di tale possibilità fa tuttavia emergere una serie di lacune e difficoltà. In particolare essa comporta che i dati API, per quanto rilevanti a fini di contrasto, non siano sempre raccolti e trasferiti dai vettori aerei per queste finalità. Comporta inoltre che, quando gli Stati membri si avvalgono di tale possibilità, i vettori aerei debbano ottemperare, a norma del diritto nazionale, a requisiti divergenti per quanto riguarda i tempi e le modalità di raccolta e trasferimento dei dati API per detta finalità. Oltre a imporre ai vettori aerei costi e complicazioni inutili, tali divergenze vanno a scapito della sicurezza interna dell'Unione e di una cooperazione efficace tra le autorità di contrasto

²⁶ GU C [...] del [...], pag. [...].

²⁷ Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate (GU L 261 del 6.8.2004, pag. 24).

competenti degli Stati membri. Inoltre, dato che l'agevolazione dei controlli di frontiera e il contrasto della criminalità sono finalità di natura diversa, è opportuno istituire un quadro giuridico distinto per la raccolta e il trasferimento dei dati API in relazione a ciascuna di esse.

- (3) La direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio²⁸ stabilisce norme sull'uso dei dati PNR a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Ai sensi di tale direttiva, gli Stati membri devono adottare i provvedimenti necessari affinché i vettori aerei trasferiscano i dati PNR, compresi i dati API raccolti, all'unità d'informazione sui passeggeri ("UIP") nazionale istituita ai sensi di tale direttiva nel caso in cui abbiano già raccolto tali dati nel normale svolgimento della loro attività. Di conseguenza, la direttiva non garantisce che i dati API siano raccolti e trasferiti in tutti i casi, in quanto i vettori aerei non hanno alcuna finalità commerciale che li induca a raccogliere una serie completa di tali dati. È importante garantire che le UIP ricevano i dati API insieme ai dati PNR, in quanto il trattamento congiunto di tali dati è necessario per permettere alle autorità di contrasto competenti degli Stati membri di prevenire, accertare, indagare e perseguire efficacemente i reati di terrorismo e i reati gravi. In particolare, il trattamento congiunto consente di identificare con precisione i passeggeri che tali autorità potrebbero dovere esaminare ulteriormente, in conformità del diritto applicabile. La suddetta direttiva, inoltre, non specifica con precisione quali informazioni costituiscano dati API. Per tali motivi è opportuno stabilire norme complementari che impongano ai vettori aerei di raccogliere e successivamente trasferire una serie specificamente definita di dati API, norme che dovrebbero applicarsi nel caso in cui i vettori aerei siano tenuti, a norma della direttiva, a raccogliere e trasferire i dati PNR sullo stesso volo.
- (4) È pertanto necessario stabilire norme chiare, armonizzate ed efficaci a livello dell'Unione sulla raccolta e sul trasferimento dei dati API a fini di prevenzione, accertamento, indagine e azione penale relativamente ai reati di terrorismo e ai reati gravi.
- (5) Tenuto conto dello stretto legame esistente tra i due atti, il presente regolamento dovrebbe essere inteso come un'integrazione delle norme della direttiva (UE) 2016/681. Pertanto i dati API dovrebbero essere raccolti e trasferiti conformemente ai requisiti specifici del presente regolamento, anche per quanto riguarda le circostanze e le modalità. Tuttavia le norme di tale direttiva si applicano a materie non specificamente disciplinate dal presente regolamento, in particolare al successivo trattamento dei dati API ricevuti dalle UIP, allo scambio di informazioni tra Stati membri, alle condizioni di accesso da parte dell'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), ai trasferimenti verso paesi terzi, alla conservazione e anonimizzazione, nonché alla protezione dei dati personali. Nella misura in cui si applicano tali norme, si applicano anche le norme della direttiva citata relative alle sanzioni e alle autorità nazionali di controllo. Il presente regolamento dovrebbe lasciare impregiudicate tali norme.
- (6) La raccolta e il trasferimento dei dati API incidono sulla vita privata delle persone fisiche e comportano il trattamento di dati personali. Per rispettare pienamente i diritti

²⁸ Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (GU L 119 del 4.5.2016, pag. 132).

fondamentali, in particolare il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, conformemente alla Carta dei diritti fondamentali dell'Unione europea ("Carta"), occorre stabilire limiti e garanzie adeguati. In particolare il trattamento dei dati API, specialmente quelli che costituiscono dati personali, dovrebbe rimanere limitato a quanto necessario e proporzionato per il conseguimento degli obiettivi perseguiti dal presente regolamento. Occorre inoltre garantire che i dati API raccolti e trasferiti ai sensi del presente regolamento non comportino alcuna forma di discriminazione vietata dalla Carta.

- (7) Dato che il presente regolamento è complementare alla direttiva (UE) 2016/681, gli obblighi dei vettori aerei da esso previsti dovrebbero applicarsi a tutti i voli per i quali gli Stati membri sono tenuti ad imporre ai vettori aerei di trasmettere i dati PNR ai sensi della direttiva (UE) 2016/681, vale a dire i voli sia di linea che non di linea sia tra Stati membri e paesi terzi (voli extra-UE) sia tra diversi Stati membri (voli intra-UE), nella misura in cui tali voli siano stati selezionati conformemente alla direttiva (UE) 2016/681, indipendentemente dal luogo di stabilimento dei vettori aerei che li effettuano.
- (8) Di conseguenza, dato che la direttiva (UE) 2016/681 non si applica ai voli nazionali, vale a dire ai voli che partono e atterrano nel territorio dello stesso Stato membro senza scali nel territorio di un altro Stato membro o di un paese terzo, e tenuto conto della dimensione transnazionale dei reati di terrorismo e dei reati gravi contemplati dal presente regolamento, tali voli non dovrebbero rientrare nell'ambito di applicazione del presente regolamento. Il presente regolamento non dovrebbe intendersi tale da pregiudicare la possibilità per gli Stati membri di imporre ai vettori aerei, ai sensi del loro diritto nazionale e nel rispetto del diritto dell'Unione, l'obbligo di raccogliere e trasferire dati API su tali voli nazionali.
- (9) Considerata la stretta relazione tra gli atti normativi dell'Unione in questione e a fini di uniformità e coerenza, è opportuno allineare il più possibile le definizioni di cui al presente regolamento a quelle di cui alla direttiva (UE) 2016/681 e al regolamento (UE) [API per la gestione delle frontiere] e interpretarle e applicarle alla luce di queste ultime²⁹.
- (10) In particolare le informazioni, relative tanto al singolo viaggiatore quanto al volo, che costituiscono congiuntamente i dati API da raccogliere e successivamente trasferire a norma del presente regolamento dovrebbero essere quelle elencate in modo chiaro ed esaustivo nel regolamento (UE) [API per la gestione delle frontiere]. A norma di detto regolamento, le informazioni di volo dovrebbero comprendere informazioni sul valico di frontiera di ingresso nel territorio dello Stato membro interessato solo ove applicabile, vale a dire non quando i dati API si riferiscono a voli intra-UE.
- (11) Per garantire un approccio il più possibile coerente alla raccolta e al trasferimento dei dati API da parte dei vettori aerei, le norme stabilite nel presente regolamento dovrebbero essere allineate, se del caso, a quelle stabilite nel regolamento (UE) [API per la gestione delle frontiere]. Ciò riguarda, in particolare, le norme sulla qualità dei dati, l'uso di mezzi automatizzati per la raccolta da parte dei vettori aerei, le modalità precise con cui essi trasferiscono al router i dati API raccolti e la cancellazione dei dati API.

²⁹ GU C [...] del [...], pag. [...].

- (12) Al fine di garantire il trattamento congiunto dei dati API e dei dati PNR per un contrasto efficace del terrorismo e dei reati gravi nell'Unione e, nel contempo, ridurre al minimo l'ingerenza nei diritti fondamentali dei passeggeri tutelati dalla Carta, le UIP dovrebbero essere le autorità competenti degli Stati membri incaricate di ricevere, e in seguito trattare ulteriormente e proteggere, i dati API raccolti e trasferiti a norma del presente regolamento. Per migliorare l'efficienza e ridurre al minimo i rischi per la sicurezza, il router, quale progettato, sviluppato, ospitato e tecnicamente mantenuto dall'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) in conformità del regolamento (UE) [API per la gestione delle frontiere], dovrebbe trasmettere alle UIP pertinenti i dati API raccolti e ad esso trasferiti dai vettori aerei a norma del presente regolamento. Visto il livello di protezione necessario per i dati API che costituiscono dati personali, anche per garantire la riservatezza delle informazioni in essi contenute, è opportuno che i dati API siano trasmessi dal router alle UIP pertinenti in modo automatizzato.
- (13) L'UIP dello Stato membro nel cui territorio atterrerà o dal cui territorio partirà il volo dovrebbe ricevere dal router i dati API per tutti i voli extra-UE, dato che per tutti questi voli sono raccolti i dati PNR conformemente alla direttiva (UE) 2016/681. Il router dovrebbe identificare il volo e le UIP corrispondenti utilizzando le informazioni contenute nel codice PNR di identificazione della pratica che, in quanto elemento di dati comune alle serie di dati API e PNR, consente alle UIP il trattamento congiunto dei dati API e PNR.
- (14) Per quanto riguarda i voli intra-UE, in linea con la giurisprudenza della Corte di giustizia dell'Unione europea, al fine di evitare ingerenze indebite nei diritti fondamentali pertinenti tutelati dalla Carta e di garantire il rispetto degli obblighi previsti dal diritto dell'Unione in materia di libera circolazione delle persone e abolizione dei controlli alle frontiere interne, è opportuno prevedere un approccio selettivo. Vista l'importanza di garantire che i dati API possano essere trattati insieme ai dati PNR, tale approccio dovrebbe essere allineato a quello della direttiva (UE) 2016/681. Pertanto i dati API relativi a detti voli dovrebbero essere trasmessi dal router alle UIP pertinenti solo se gli Stati membri hanno selezionato i voli in questione in applicazione dell'articolo 2 della direttiva (UE) 2016/681. Come ricordato dalla Corte di giustizia dell'Unione europea, la selezione implica che gli Stati membri debbano applicare gli obblighi in questione solo per quanto riguarda, tra l'altro, determinati collegamenti o modalità di viaggio o certi aeroporti, fatto salvo il riesame periodico della selezione stessa.
- (15) Per consentire l'applicazione di tale approccio selettivo a norma del presente regolamento riguardo ai voli intra-UE, gli Stati membri dovrebbero essere tenuti a redigere e trasmettere a eu-LISA gli elenchi dei voli selezionati, in modo che eu-LISA possa garantire che il router trasmetta alle UIP pertinenti solo i dati API relativi a tali voli e che quelli relativi agli altri voli intra-UE siano immediatamente cancellati in via definitiva.
- (16) Per evitare che sia compromessa, in particolare per rischi di elusione, l'efficacia del sistema basato sulla raccolta e sul trasferimento dei dati API istituito dal presente regolamento e dei dati PNR nell'ambito del sistema istituito dalla direttiva (UE) 2016/681 al fine di prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi, la selezione dei voli intra-UE da parte degli Stati membri dovrebbe essere considerata un'informazione riservata. Pertanto tale informazione non dovrebbe essere condivisa con i vettori aerei, i quali dovrebbero essere tenuti a raccogliere i dati API su tutti i voli contemplati dal presente regolamento, compresi

tutti i voli intra-UE, e a trasferirli in seguito al router, dove dovrebbe essere messa in atto la necessaria selezione. Inoltre, il fatto di raccogliere i dati API su tutti i voli intra-UE impedisce ai passeggeri di sapere quali dati API di voli intra-UE selezionati, e quindi quali dati PNR, siano trasmessi alle UIP conformemente alla valutazione degli Stati membri. Tale approccio garantisce anche che eventuali modifiche della selezione possano essere effettuate in modo rapido ed efficace, senza imporre ai vettori aerei oneri economici e operativi indebiti.

- (17) Per garantire il rispetto del diritto fondamentale alla protezione dei dati personali e in linea con il regolamento (UE) [API per la gestione delle frontiere], il presente regolamento dovrebbe identificare i titolari del trattamento. Ai fini di un monitoraggio efficace, che garantisca un'adeguata protezione dei dati personali e riduca al minimo i rischi per la sicurezza, dovrebbero inoltre essere previste norme in materia di registrazione, sicurezza del trattamento e autocontrollo. Laddove riguardino il trattamento di dati personali, tali disposizioni dovrebbero essere intese come complementari agli atti generalmente applicabili del diritto dell'Unione in materia di protezione dei dati personali, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio³⁰, la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio³¹ e il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio³². Il presente regolamento dovrebbe lasciare impregiudicati tali atti, che si applicano anche al trattamento dei dati personali ai sensi del presente regolamento conformemente alle sue disposizioni.
- (18) Il router da creare e gestire a norma del regolamento (UE) [API per la gestione delle frontiere] dovrebbe ridurre e semplificare le connessioni tecniche necessarie per trasferire i dati API, limitandole a un'unica connessione per vettore aereo e per UIP. Pertanto il presente regolamento fa obbligo a ogni UIP e ogni vettore aereo di stabilire una connessione con il router e di conseguire la necessaria integrazione con lo stesso, in modo da garantire il corretto funzionamento del sistema di trasferimento dei dati API istituito dal presente regolamento.
- (19) Considerati gli interessi dell'Unione in gioco, i costi adeguati sostenuti dagli Stati membri in relazione alle loro connessioni e alla loro integrazione con il router a norma del presente regolamento dovrebbero essere a carico del bilancio dell'Unione, conformemente alla legislazione applicabile e fatte salve alcune eccezioni. I costi coperti da tali eccezioni dovrebbero essere sostenuti dallo Stato membro interessato.
- (20) A norma del regolamento (UE) 2018/1726, gli Stati membri possono incaricare eu-LISA di agevolare la connettività con i vettori aerei al fine di assistere gli Stati

³⁰ 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 (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

³¹ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

³² Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

membri nell'attuazione della direttiva (UE) 2016/681, in particolare raccogliendo e trasferendo dati PNR tramite il router.

- (21) Non si può escludere che, a causa di circostanze eccezionali e nonostante l'adozione di tutte le misure ragionevoli a norma del presente regolamento e, per quanto riguarda il router, del regolamento (UE) [API per la gestione delle frontiere], il router o i sistemi o le infrastrutture che lo collegano alle UIP e ai vettori aerei non funzionino correttamente, con conseguente impossibilità tecnica di utilizzare il router per trasmettere i dati API. Data l'indisponibilità del router e il fatto che in generale non sarà ragionevolmente possibile per i vettori aerei trasferire i dati API interessati dal guasto in modo lecito, sicuro, efficace e rapido con mezzi alternativi, l'obbligo per i vettori aerei di trasferire tali dati API al router dovrebbe cessare di applicarsi fintanto che persiste l'impossibilità tecnica. In tal caso le parti interessate dovrebbero informarsi immediatamente a vicenda e adottare immediatamente tutte le misure necessarie per porre rimedio all'impossibilità tecnica, al fine di ridurre al minimo la durata e le conseguenze negative. Tale disposizione dovrebbe lasciare impregiudicati l'obbligo imposto dal presente regolamento a tutte le parti interessate di garantire il corretto funzionamento del router e dei rispettivi sistemi e infrastrutture, nonché l'imposizione di sanzioni ai vettori aerei in caso di mancato rispetto di tali obblighi, anche quando applicano detta disposizione in casi ingiustificati. Per scoraggiare tali usi impropri e facilitare il controllo e, se necessario, l'imposizione di sanzioni, i vettori aerei che applicano detta disposizione in caso di guasti del proprio sistema e della propria infrastruttura dovrebbero riferire in merito all'autorità di controllo competente.
- (22) È opportuno prevedere che siano designate e abilitate autorità nazionali incaricate del controllo delle norme del presente regolamento, così da garantire che siano effettivamente applicate dai vettori aerei. Le disposizioni del presente regolamento relative a tale controllo, anche per quanto riguarda l'imposizione di sanzioni ove necessario, dovrebbero lasciare impregiudicati i compiti e i poteri delle autorità di controllo istituite a norma del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680, anche in relazione al trattamento dei dati personali a norma del presente regolamento.
- (23) È opportuno che gli Stati membri prevedano sanzioni effettive proporzionate e dissuasive, anche pecuniarie, a carico dei vettori aerei che non si conformano agli obblighi in materia di raccolta e trasferimento dei dati API ai sensi del presente regolamento.
- (24) Per adottare misure riguardanti i requisiti tecnici e le norme operative per i mezzi automatizzati di raccolta dei dati API leggibili meccanicamente, i protocolli comuni e i formati da utilizzare per il trasferimento dei dati API a cura dei vettori aerei, le norme tecniche e procedurali per la trasmissione dei dati API dal router alle UIP e le connessioni e l'integrazione delle UIP e dei vettori aerei con il router, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea riguardo, rispettivamente, agli articoli 4, 5, 10 e 11. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016³³. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti

³³ GU L 123 del 12.5.2016, pag. 1.

contemporaneamente agli esperti degli Stati membri e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

- (25) Tutte le parti interessate, in particolare i vettori aerei e le UIP, dovrebbero avere il tempo sufficiente per compiere i preparativi necessari ad ottemperare ai rispettivi obblighi stabiliti dal presente regolamento, tenendo conto del fatto che alcuni di questi preparativi, come quelli relativi agli obblighi in materia di connessione e integrazione con il router, potranno essere ultimati solo dopo il completamento delle fasi di progettazione e sviluppo del router stesso e una volta che quest'ultimo sarà entrato in funzione. Pertanto il presente regolamento dovrebbe applicarsi solo a decorrere da una data appropriata successiva alla data di entrata in funzione del router, specificata dalla Commissione in conformità del regolamento (UE) [API per il controllo di frontiera]. Tuttavia la Commissione dovrebbe potere adottare atti delegati a norma del presente regolamento già da una data anteriore, in modo da garantire che il sistema istituito dal presente regolamento sia operativo non appena possibile.
- (26) Gli obiettivi del presente regolamento, vale a dire contribuire alla prevenzione, all'accertamento, all'indagine e al perseguimento di reati di terrorismo e reati gravi, tenuto conto della dimensione transnazionale dei reati in questione e della necessità di cooperare su base transfrontaliera per contrastarli efficacemente, non possono essere conseguiti in misura sufficiente dai singoli Stati membri ma possono essere conseguiti meglio a livello di Unione. L'Unione può quindi intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.
- (27) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione del presente regolamento, non è da esso vincolata né è soggetta alla sua applicazione.
- (28) [A norma dell'articolo 3 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, l'Irlanda ha notificato che desidera partecipare all'adozione e all'applicazione del presente regolamento.] OPPURE [A norma degli articoli 1 e 2 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda non partecipa all'adozione del presente regolamento, non è da esso vincolata né è soggetta alla sua applicazione.]
- (29) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il [XX]³⁴,

³⁴ [GU C... del..., pag...].

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO 1

DISPOSIZIONI GENERALI

Articolo 1

OGGETTO

Al fine di prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi, il presente regolamento stabilisce norme riguardanti:

- a) la raccolta, a cura dei vettori aerei, delle informazioni anticipate sui passeggeri ("dati API") sui voli extra-UE e su voli intra-UE selezionati;
- b) il trasferimento dei dati API al router a cura dei vettori aerei;
- c) la trasmissione dal router alle unità d'informazione sui passeggeri ("UIP") dei dati API relativi ai voli extra-UE e ai voli intra-UE selezionati.

Articolo 2

Ambito di applicazione

Il presente regolamento si applica ai vettori aerei che effettuano voli extra-UE o intra-UE, di linea o non di linea.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

- a) "vettore aereo": l'impresa di trasporto aereo come definita all'articolo 3, punto 1, della direttiva (UE) 2016/681;
- b) "volo extra-UE": un volo come definito all'articolo 3, punto 2, della direttiva (UE) 2016/681;
- c) "volo intra-UE": un volo come definito all'articolo 3, punto 3, della direttiva (UE) 2016/681;
- d) "volo di linea": un volo come definito all'articolo 3, lettera e), del regolamento (UE) [API per la gestione delle frontiere];
- e) "volo non di linea": un volo come definito all'articolo 3, lettera f), del regolamento (UE) [API per la gestione delle frontiere];
- f) "passeggero": chiunque risponda alla definizione di cui all'articolo 3, punto 4, della direttiva (UE) 2016/681;
- g) "equipaggio": chiunque risponda alla definizione di cui all'articolo 3, lettera h), del regolamento (UE) [API per la gestione delle frontiere];
- h) "viaggiatore": chiunque risponda alla definizione di cui all'articolo 3, lettera i), del regolamento (UE) [API per la gestione delle frontiere];
- i) "informazioni anticipate sui passeggeri" o "dati API": i dati di cui all'articolo 3, lettera j), del regolamento (UE) [API per la gestione delle frontiere];

- j) "codice di prenotazione" o "PNR": le informazioni relative al viaggio di ciascun passeggero come definite all'articolo 3, punto 5, della direttiva (UE) 2016/681;
- k) "unità d'informazione sui passeggeri " o "UIP": l'autorità competente istituita da uno Stato membro figurante nelle notifiche e nelle relative modifiche pubblicate dalla Commissione ai sensi dell'articolo 4, paragrafi 1 e 5, rispettivamente, della direttiva (UE) 2016/681;
- l) "reato di terrorismo": un reato come definito agli articoli da 3 a 12 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio³⁵;
- m) "reato grave": un reato come definito all'articolo 3, punto 9, della direttiva (UE) 2016/681;
- n) "router": il router come definito all'articolo 3, lettera k), del regolamento (UE) [API per la gestione delle frontiere];
- o) "dati personali": le informazioni di cui all'articolo 4, punto 1, del regolamento (UE) 2016/679.

CAPO 2

TRATTAMENTO DEI DATI API

Articolo 4

Raccolta, trasferimento e cancellazione dei dati API a cura dei vettori aerei

1. I vettori aerei raccolgono i dati API dei viaggiatori sui voli di cui all'articolo 2 al fine di trasferirli al router conformemente all'articolo 6. Qualora il volo sia operato in code-sharing da uno o più vettori aerei, l'obbligo di trasferire i dati API spetta al vettore aereo che opera il volo.
2. I vettori aerei raccolgono i dati API in modo tale che i dati API che trasferiscono conformemente al paragrafo 6 siano esatti, completi e aggiornati.
3. I vettori aerei raccolgono i dati API di cui all'articolo 4, paragrafo 2, lettere da a) a d), del regolamento (UE) [API per la gestione delle frontiere] ricorrendo a mezzi automatizzati per raccogliere i dati del documento di viaggio del viaggiatore interessato leggibili meccanicamente. La raccolta è conforme ai requisiti tecnici e alle norme operative dettagliati di cui al paragrafo 5, ove tali norme siano state adottate e siano applicabili.

Tuttavia, se è impossibile usare tali mezzi automatizzati perché i documenti di viaggio non contengono dati leggibili meccanicamente, i vettori aerei raccolgono i dati manualmente, in modo tale da garantire il rispetto del paragrafo 2.
4. I mezzi automatizzati usati dai vettori aerei per raccogliere i dati API conformemente al presente regolamento sono affidabili, sicuri e aggiornati.

³⁵ Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio (GU L 88 del 31.3.2017, pag. 6).

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 19 per integrare il presente regolamento stabilendo requisiti tecnici e norme operative dettagliati per la raccolta dei dati API di cui all'articolo 4, paragrafo 2, lettere da a) a d), del regolamento (UE) [API per la gestione delle frontiere] conformemente ai paragrafi 3 e 4 del presente articolo.
6. I vettori aerei trasferiscono al router, con mezzi automatizzati, i dati API raccolti conformemente al paragrafo 1. Il trasferimento è conforme alle norme dettagliate di cui al paragrafo 9, ove tali norme siano state adottate e siano applicabili.
7. I vettori aerei trasferiscono i dati API sia al momento del check-in che immediatamente dopo la chiusura del volo, vale a dire una volta che i viaggiatori sono saliti a bordo dell'aeromobile pronto per la partenza e non è più possibile l'imbarco o lo sbarco di viaggiatori.
8. Fatta salva la possibilità per i vettori aerei di conservare e utilizzare i dati ove necessario per il normale svolgimento della loro attività in conformità del diritto applicabile, i vettori aerei provvedono immediatamente a correggere, completare, aggiornare o cancellare in via definitiva i dati API in questione in entrambe le situazioni seguenti:
 - a) qualora si rendano conto che i dati API raccolti sono inesatti, incompleti, non aggiornati o trattati illecitamente, o che i dati trasferiti non costituiscono dati API;
 - b) qualora sia stato completato il trasferimento dei dati API conformemente al paragrafo 3.

Se si rendono conto della situazione di cui al primo comma, lettera a), dopo aver completato il trasferimento dei dati a norma del paragrafo 6, i vettori aerei ne informano immediatamente l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA). Non appena riceve l'informazione eu-LISA la comunica immediatamente alle UIP che hanno ricevuto i dati API trasmessi tramite il router.

9. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 19 per integrare il presente regolamento stabilendo le norme dettagliate necessarie sui protocolli comuni e sui formati di dati supportati da usare per il trasferimento dei dati API al router di cui al paragrafo 6.

Articolo 5

Trasmissione dei dati API dal router alle UIP

1. Il router trasmette immediatamente e in maniera automatizzata i dati API ad esso trasferiti dai vettori aerei a norma dell'articolo 4 alle UIP dello Stato membro nel cui territorio atterrerà o dal cui territorio partirà il volo, o a entrambi gli Stati membri in questione nel caso di voli intra-UE. Qualora un volo faccia uno o più scali nel territorio di Stati membri diversi da quello da cui è partito, il router trasmette i dati API alle UIP di tutti gli Stati membri interessati.

Ai fini di tale trasmissione eu-LISA istituisce e tiene aggiornata una tabella di corrispondenza tra i diversi aeroporti di origine e di destinazione, indicante anche i paesi a cui appartengono.

Tuttavia, per i voli intra-UE il router trasmette i dati API all'UIP solo per quanto riguarda i voli inclusi nell'elenco di cui al paragrafo 2.

Il router trasmette i dati API secondo le norme dettagliate di cui al paragrafo 3, ove tali norme siano state adottate e siano applicabili.2. Ciascuno degli Stati membri che decidono di applicare la direttiva (UE) 2016/681 ai voli intra-UE conformemente all'articolo 2 di tale direttiva redige un elenco dei voli intra-UE interessati ed entro la data di applicazione del presente regolamento di cui all'articolo 21, secondo comma, lo trasmette a eu-LISA. Conformemente all'articolo 2 di tale direttiva, detti Stati membri riesaminano e, se necessario, aggiornano periodicamente gli elenchi e trasmettono immediatamente a eu-LISA gli eventuali elenchi aggiornati. Le informazioni contenute in tali elenchi sono trattate in modo riservato.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 19 per integrare il presente regolamento stabilendo le norme tecniche e procedurali dettagliate necessarie per la trasmissione dei dati API dal router di cui al paragrafo 1.

CAPO 3

REGISTRAZIONE, PROTEZIONE DEI DATI PERSONALI E SICUREZZA

Articolo 6

Registrazioni

1. I vettori aerei creano registrazioni di tutte le operazioni di trattamento a norma del presente regolamento effettuate con i mezzi automatizzati di cui all'articolo 4, paragrafo 3. Tali registrazioni riguardano la data, l'ora e il luogo di trasferimento dei dati API.
2. Le registrazioni di cui al paragrafo 1 sono usate solo per garantire la sicurezza e l'integrità dei dati API e la liceità del trattamento, in particolare per quanto riguarda la conformità alle disposizioni di cui al presente regolamento, compresi i procedimenti sanzionatori applicabili per violazione di tali disposizioni conformemente agli articoli 15 e 16.
3. I vettori aerei adottano misure adeguate per proteggere le registrazioni da essi create a norma del paragrafo 1 dall'accesso non autorizzato e da altri rischi per la sicurezza.
4. I vettori aerei conservano le registrazioni da essi create a norma del paragrafo 1 per un anno dal momento della creazione. Alla scadenza di tale periodo essi cancellano immediatamente le registrazioni in via definitiva.

Tuttavia, se le registrazioni sono necessarie per le procedure volte a monitorare o garantire la sicurezza e l'integrità dei dati API o la liceità delle operazioni di trattamento di cui al paragrafo 2 e se tali procedure sono già iniziate alla scadenza del periodo di cui al primo comma, i vettori aerei possono conservare le registrazioni per il tempo necessario al completamento di tali procedure. In tal caso, essi cancellano immediatamente le registrazioni quando non sono più necessarie per tali procedure.

Articolo 7

Titolari del trattamento dei dati personali

Le UIP sono titolari del trattamento ai sensi dell'articolo 3, punto 8, della direttiva (UE) 2016/680, in relazione al trattamento tramite il router dei dati API che costituiscono dati personali ai sensi del presente regolamento, comprese la trasmissione e la conservazione di tali dati sul router per motivi tecnici.

I vettori aerei sono titolari del trattamento ai sensi dell'articolo 4, punto 7, del regolamento (UE) 2016/679, per il trattamento dei dati API che costituiscono dati personali in relazione alla loro raccolta e al loro trasferimento al router a norma del presente regolamento.

Articolo 8

Sicurezza

Le UIP e i vettori aerei garantiscono la sicurezza dei dati API, in particolare di quelli che costituiscono dati personali, che essi trattano a norma del presente regolamento.

Le UIP e i vettori aerei cooperano tra loro e con eu-LISA, secondo le rispettive responsabilità e nel rispetto del diritto dell'Unione, per garantire tale sicurezza.

Articolo 9

Verifica interna

I vettori aerei e le UIP controllano l'ottemperanza ai rispettivi obblighi ai sensi del presente regolamento, in particolare per quanto riguarda il trattamento dei dati API che costituiscono dati personali, anche attraverso la verifica frequente delle registrazioni a norma dell'articolo 7.

CAPO 4

DISPOSIZIONI RELATIVE AL ROUTER

Articolo 10

Connessione delle UIP al router

1. Gli Stati membri provvedono affinché le loro UIP siano connesse al router. Essi provvedono affinché i loro sistemi e infrastrutture nazionali per il ricevimento e l'ulteriore trattamento dei dati API trasferiti a norma del presente regolamento siano integrati con il router.

Gli Stati membri provvedono affinché la connessione e l'integrazione con il router consentano alle loro UIP di ricevere e trattare ulteriormente i dati API, nonché di scambiare qualsiasi comunicazione ad essi relativa, in modo lecito, sicuro, efficace e rapido.

2. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 19 per integrare il presente regolamento stabilendo le norme dettagliate necessarie per le connessioni e l'integrazione con il router di cui al paragrafo 1.

Articolo 11

Connessione dei vettori aerei al router

1. I vettori aerei garantiscono la loro connessione al router. Essi provvedono affinché i loro sistemi e infrastrutture per il trasferimento dei dati API al router a norma del presente regolamento siano integrati con il router.

I vettori aerei provvedono affinché la connessione e l'integrazione con il router consentano loro di trasferire i dati API, nonché di scambiare tutte le comunicazioni ad essi relative, in modo lecito, sicuro, efficace e rapido.

2. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 19 per integrare il presente regolamento stabilendo le norme dettagliate necessarie per le connessioni e l'integrazione con il router di cui al paragrafo 1.

Articolo 12

Spese a carico degli Stati membri

1. Le spese sostenute dagli Stati membri per la connessione e l'integrazione con il router di cui all'articolo 10 sono a carico del bilancio generale dell'Unione.

Sono escluse e sono a carico degli Stati membri le spese seguenti:

- a) spese per la gestione del progetto, compresi riunioni, missioni e uffici;
 - b) spese per l'hosting dei sistemi di tecnologie dell'informazione (IT) nazionali, compresi spazi, implementazione, elettricità e impianti di raffreddamento;
 - c) spese per la gestione dei sistemi IT nazionali, compresi operatori e contratti di assistenza;
 - d) spese per la progettazione, lo sviluppo, l'implementazione, il funzionamento e la manutenzione delle reti di comunicazione nazionali.
2. Sono a carico degli Stati membri anche le spese derivanti dalla gestione, dall'utilizzo e dalla manutenzione delle loro connessioni al router e dall'integrazione con quest'ultimo.

Articolo 13

Azioni in caso di impossibilità tecnica di usare il router

1. Qualora, a causa di un guasto del router, sia tecnicamente impossibile utilizzarlo per trasmettere i dati API, eu-LISA ne informa immediatamente i vettori aerei e le UIP in maniera automatizzata. In tal caso eu-LISA adotta immediatamente misure per rimediare all'impossibilità tecnica di usare il router e, una volta risolto il problema, ne informa immediatamente dette parti.

Nel periodo che intercorre tra tali notifiche non si applica l'articolo 4, paragrafo 6, in quanto l'impossibilità tecnica impedisce il trasferimento dei dati API al router. Analogamente, qualora ciò si verifici, l'articolo 4, paragrafo 1, non si applica in tale periodo ai dati API in questione.

2. Qualora, a causa di un guasto dei sistemi o delle infrastrutture di uno Stato membro di cui all'articolo 10, sia tecnicamente impossibile utilizzare il router per trasmettere i dati API, l'UIP di tale Stato membro ne informa immediatamente i vettori aerei, le altre UIP, eu-LISA e la Commissione in maniera automatizzata. In tal caso lo Stato

membro adotta immediatamente misure per rimediare all'impossibilità tecnica di usare il router e, una volta risolto il problema, ne informa immediatamente dette parti.

Nel periodo che intercorre tra tali notifiche non si applica l'articolo 4, paragrafo 6, in quanto l'impossibilità tecnica impedisce il trasferimento dei dati API al router. Analogamente, qualora ciò si verifichi, l'articolo 4, paragrafo 1, non si applica in tale periodo ai dati API in questione.

3. Qualora, a causa di un guasto dei sistemi o delle infrastrutture di un vettore aereo di cui all'articolo 11, sia tecnicamente impossibile utilizzare il router per trasmettere i dati API, il vettore aereo ne informa immediatamente le UIP, eu-LISA e la Commissione in maniera automatizzata. In tal caso il vettore aereo adotta immediatamente misure per rimediare all'impossibilità tecnica di usare il router e, una volta risolto il problema, ne informa immediatamente dette parti.

Nel periodo che intercorre tra tali notifiche non si applica l'articolo 4, paragrafo 6, in quanto l'impossibilità tecnica impedisce il trasferimento dei dati API al router. Analogamente, qualora ciò si verifichi, l'articolo 4, paragrafo 1, non si applica in tale periodo ai dati API in questione.

Una volta risolta l'impossibilità tecnica, il vettore aereo interessato presenta senza ritardo all'autorità nazionale di controllo competente di cui all'articolo 15 una relazione contenente tutti i dettagli necessari su tale impossibilità tecnica, compresi i motivi, la portata e le conseguenze, nonché le misure adottate per porvi rimedio.

Articolo 14

Responsabilità relative al router

Lo Stato membro o il vettore aereo è responsabile di ogni eventuale danno arrecato al router conseguente all'inosservanza degli obblighi di cui al presente regolamento, a meno che e nella misura in cui eu-LISA abbia omissso di adottare provvedimenti ragionevolmente idonei a prevenire il danno o ridurne al minimo l'impatto.

CAPO 5

CONTROLLO, SANZIONI E MANUALE

Articolo 15

Autorità nazionale di controllo

1. Gli Stati membri designano una o più autorità nazionali di controllo incaricate di monitorare, nel loro territorio, l'applicazione delle disposizioni del presente regolamento da parte dei vettori aerei e di garantirne l'osservanza.
2. Gli Stati membri provvedono affinché le autorità nazionali di controllo dispongano di tutti i mezzi e i poteri di indagine e di esecuzione necessari per svolgere i loro compiti a norma del presente regolamento, anche imponendo, se del caso, le sanzioni di cui all'articolo 16. Essi stabiliscono norme dettagliate relative all'esecuzione di tali compiti e all'esercizio di tali poteri, assicurando che l'esecuzione e l'esercizio in questione siano effettivi, proporzionati e dissuasivi e siano soggetti a garanzie nel rispetto dei diritti fondamentali garantiti dal diritto dell'Unione.

3. Entro la data di applicazione del presente regolamento di cui all'articolo 21, secondo comma, gli Stati membri comunicano alla Commissione il nome e i dati di contatto delle autorità designate a norma del paragrafo 1 e le norme dettagliate stabilite a norma del paragrafo 2. Essi informano la Commissione senza ritardo di ogni successivo cambiamento o modifica di quanto sopra.
4. Il presente articolo non pregiudica i poteri delle autorità di controllo di cui all'articolo 51 del regolamento (UE) 2016/679 e all'articolo 41 della direttiva (UE) 2016/680.

Articolo 16

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni da applicare in caso di violazione del presente regolamento e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste sono effettive, proporzionate e dissuasive.

Gli Stati membri notificano tali norme e misure alla Commissione entro la data di applicazione del presente regolamento di cui all'articolo 21, secondo comma, e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

Articolo 17

Manuale pratico

La Commissione, in stretta cooperazione con le UIP, le altre autorità competenti degli Stati membri, i vettori aerei e le agenzie competenti dell'Unione, redige e mette a disposizione del pubblico un manuale pratico contenente orientamenti, raccomandazioni e buone prassi per l'attuazione del presente regolamento.

Il manuale pratico tiene conto dei manuali pertinenti esistenti.

La Commissione adotta il manuale pratico sotto forma di raccomandazione.

CAPO 6

RELAZIONE CON ALTRI STRUMENTI VIGENTI

Articolo 18

Modifiche del regolamento (UE) 2019/818

All'articolo 39, i paragrafi 1 e 2 sono sostituiti dai seguenti:

"1. È istituito un archivio centrale di relazioni e statistiche (CRRS) al fine di sostenere gli obiettivi del SIS, dell'Eurodac e dell'ECRIS-TCN, in conformità dei rispettivi strumenti giuridici che disciplinano tali sistemi, e fornire dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati. Il CRRS sostiene inoltre gli obiettivi del regolamento (UE).../... del Parlamento europeo e del Consiglio* [*il presente regolamento*].

* Regolamento (UE) [numero] del Parlamento europeo e del Consiglio, del xy, relativo [titolo adottato ufficialmente] (GU L ...).

2. eu-LISA istituisce, attua e ospita nei suoi siti tecnici il CRRS contenente i dati e le statistiche di cui all'articolo 74 del regolamento (UE) 2018/1862 e all'articolo 32 del regolamento (UE) 2019/816, separati per logica in base al sistema di informazione dell'UE. eu-LISA raccoglie inoltre i dati e le statistiche estratti dal router di cui all'articolo 13, paragrafo 1, del regolamento (UE).../... * [il presente regolamento]. L'accesso al CRRS è concesso mediante un accesso controllato e sicuro e specifici profili di utente, unicamente a fini di elaborazione di relazioni e statistiche, alle autorità di cui all'articolo 74 del regolamento (UE) 2018/1862, all'articolo 32 del regolamento (UE) 2019/816 e all'articolo 13, paragrafo 1, del regolamento (UE) .../...* [il presente regolamento].".

CAPO 7

DISPOSIZIONI FINALI

Articolo 19

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.
2. Il potere di adottare gli atti delegati di cui all'articolo 4, paragrafi 5 e 9, all'articolo 5, paragrafo 3, all'articolo 10, paragrafo 2, e all'articolo 11, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal [data di adozione del presente regolamento]. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.
3. La delega di potere di cui all'articolo 4, paragrafi 5 e 9, all'articolo 5, paragrafo 3, all'articolo 10, paragrafo 2, e all'articolo 11, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.
4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.
5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

Articolo 20

Monitoraggio e valutazione

1. Entro [quattro anni dalla data di entrata in vigore del presente regolamento] e successivamente ogni quattro anni, la Commissione elabora una relazione contenente una valutazione globale del presente regolamento, comprendente una valutazione di quanto segue:
 - a) l'applicazione del presente regolamento;
 - b) la misura in cui il presente regolamento ha conseguito i suoi obiettivi;
 - c) l'impatto del presente regolamento sui diritti fondamentali tutelati dal diritto dell'Unione.
 - d) La Commissione presenta la relazione di valutazione al Parlamento europeo, al Consiglio, al Garante europeo della protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali. Se del caso, alla luce della valutazione condotta, la Commissione presenta al Parlamento europeo e al Consiglio una proposta legislativa intesa a modificare il presente regolamento.
2. Gli Stati membri e i vettori aerei comunicano alla Commissione, su richiesta, le informazioni necessarie per redigere le relazioni di cui al paragrafo 1. Tuttavia, gli Stati membri possono astenersi dal fornire tali informazioni se necessario, e nella debita misura, per non divulgare metodi di lavoro riservati o non compromettere le indagini delle loro UIP o altre autorità di contrasto in corso. La Commissione garantisce che tutte le informazioni riservate comunicate siano adeguatamente protette.

Articolo 21

Entrata in vigore e applicazione

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a decorrere da due anni dopo l'entrata in funzione del router, specificata dalla Commissione conformemente all'articolo 27 del regolamento (UE) [API per la gestione delle frontiere].

Tuttavia, l'articolo 4, paragrafi 5 e 9, l'articolo 5, paragrafo 3, l'articolo 10, paragrafo 2, l'articolo 11, paragrafo 2, e l'articolo 19 si applicano a decorrere da [data di entrata in vigore del presente regolamento].

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri conformemente ai trattati.

Fatto a Strasburgo, il

Per il Parlamento europeo
La presidente

Per il Consiglio
Il presidente

SCHEDA FINANZIARIA LEGISLATIVA

Le implicazioni finanziarie della presente proposta sono coperte dalla scheda finanziaria legislativa congiunta allegata alla proposta di regolamento (UE) [API per la gestione delle frontiere].