

# CAMERA DEI DEPUTATI

---

N.518

## **ATTO DEL GOVERNO SOTTOPOSTO A PARERE PARLAMENTARE**

Schema di decreto legislativo recante attuazione della direttiva (UE) 2016/681 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 (518)

*(articoli 1 e 12 della legge 25 ottobre 2017, n. 163)*

---

*Trasmesso alla Presidenza il 21 febbraio 2018*

---

SCHEMA DI DECRETO LEGISLATIVO RECANTE ATTUAZIONE DELLA 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, E DISCIPLINA DELL'OBBLIGO PER I VETTORI DI COMUNICARE I DATI RELATIVI ALLE PERSONE TRASPORTATE IN ATTUAZIONE DELLA DIRETTIVA 2004/82/CE DEL CONSIGLIO DEL 29 APRILE 2004

Visti gli articoli 76 e 87 della Costituzione;

Vista la direttiva (UE) n. 2016/681/UE 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;

Vista la decisione di esecuzione (UE) 2017/759 della Commissione del 28 aprile 2017, sui protocolli comuni e i formati dei dati che i vettori aerei devono utilizzare per trasferire i dati PNR alle Unità di informazione sui passeggeri;

Visto il decreto legislativo 2 agosto 2007, n. 144, recante attuazione della direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori aerei di comunicare i dati relativi alle persone trasportate;

Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016 e 2017;

Visto il regio decreto 30 marzo 1942, n. 327, recante approvazione del testo definitivo del Codice della navigazione, e successive modificazioni;

Vista la legge 1 aprile 1981, n. 121, recante il nuovo ordinamento dell'Amministrazione della pubblica sicurezza;

Vista la legge 24 novembre 1981, n. 689, recante modifiche al sistema penale;

Vista la legge 30 settembre 1993, n. 388, recante «Ratifica ed esecuzione: a) del protocollo di adesione del Governo della Repubblica italiana all'accordo di Schengen del 14 giugno 1985 tra i Governi degli Stati dell'Unione economica del Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, con due dichiarazioni comuni; b) dell'accordo di adesione della Repubblica italiana alla convenzione del 19 giugno 1990 di applicazione del summenzionato accordo di Schengen, con allegate due dichiarazioni unilaterali dell'Italia e della Francia, nonché la convenzione, il relativo atto finale, con annessi l'atto finale, il processo verbale e la dichiarazione comune dei Ministri e Segretari di Stato firmati in occasione della firma della citata convenzione del 1990, e la dichiarazione comune relativa agli articoli 2 e 3 dell'accordo di adesione summenzionato; c) dell'accordo tra il Governo della Repubblica italiana ed il Governo



della Repubblica francese relativo agli articoli 2 e 3 dell'accordo di cui alla lettera b); tutti atti firmati a Parigi il 27 novembre 1990»;

Visto il decreto legislativo 25 luglio 1997, n. 250, istitutivo dell'Ente nazionale per l'aviazione civile (ENAC);

Visto il decreto legislativo 25 luglio 1998, n. 286, recante il Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, e successive modificazioni;

Visto il decreto-legge 8 settembre 2004, n. 237, convertito, con modificazioni, dalla legge 9 novembre 2004, n. 265, recante interventi urgenti nel settore dell'aviazione civile;

Vista la legge 3 agosto 2007, n. 124, concernente il sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto;

Visto il decreto legislativo 6 settembre 2011, n. 159, recante il Codice delle leggi antimafia e delle misure di prevenzione;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione dell'8 febbraio 2018 ;

Acquisito il parere del Garante per la protezione dei dati personali, espresso nella riunione del... ;

Acquisiti i pareri delle competenti Commissioni della Camera dei Deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del... ;

Sulla proposta del Presidente del Consiglio dei Ministri e dei Ministri dell'interno e della giustizia, di concerto con i Ministri della difesa, dell'economia e delle finanze e degli affari esteri e della cooperazione internazionale

**E M A N A**

il seguente decreto legislativo

## **CAPO I**

### ***Disposizioni generali***

#### **ART. 1**

*(Oggetto e ambito di applicazione)*

1. Il presente decreto, in attuazione della 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, disciplina:

a) il trasferimento a cura dei vettori aerei dei dati del codice di prenotazione dei passeggeri (PNR) dei voli *extra-UE* e dei voli *intra-UE*;



*fr*

- b) le modalità del trattamento dei dati di cui alla lettera a), comprese le operazioni di raccolta, uso, conservazione e scambio con gli Stati membri.
2. Il presente decreto disciplina, altresì, il trattamento dei dati API trasmessi dai vettori aerei e relativi ai passeggeri che fanno ingresso nel territorio dello Stato italiano, effettuato dai competenti Uffici incaricati dei controlli di polizia di frontiera.
3. Le disposizioni del presente decreto non pregiudicano l'applicazione degli accordi o delle intese bilaterali o multilaterali sullo scambio di informazioni tra autorità competenti entrati in vigore con Stati membri dell'Unione europea entro il 24 maggio 2016, in quanto compatibili con la direttiva di cui al comma 1, né l'applicazione degli obblighi derivanti da accordi bilaterali o multilaterali conclusi con Stati non appartenenti all'Unione europea.

## ART. 2 (Definizioni)

1. Ai fini del presente decreto si intende per:

- a) «dati PNR», le informazioni relative al viaggio di ciascun passeggero consistenti nei dati di cui all'allegato I della direttiva (UE) 2016/681, necessari per il trattamento e il controllo delle prenotazioni da parte dei vettori aerei e contenuti nel codice di prenotazione. Nel caso in cui con una singola prenotazione vengano acquistati più biglietti, il PNR contiene le informazioni relative a tutti i soggetti cui la prenotazione si riferisce, siano esse registrate nei sistemi di prenotazione o di controllo delle partenze in fase di imbarco o in sistemi equivalenti dotati delle medesime funzionalità;
- b) «mascheramento dei dati», l'operazione attraverso la quale vengono resi non visibili alla consultazione le informazioni che consentono l'identificazione diretta dell'interessato;
- c) «metodo *push*», il metodo in base al quale i vettori aerei trasferiscono i dati PNR al Sistema Informativo di cui al comma 2, *lett. m*);
- d) «passeggero», chiunque, a esclusione dei membri dell'equipaggio, sia trasportato o da trasportare in un aeromobile, anche nella fase di transito o trasferimento, e risulti registrato nelle liste dei passeggeri;
- e) «reati di terrorismo», i reati di cui all'articolo 51, comma 3-*quater*, del codice di procedura penale;
- f) «reati gravi», i reati che, ai sensi della legge penale italiana, integrano le fattispecie elencate nell'allegato II della direttiva (UE) 2016/681, puniti con una pena detentiva o una misura di sicurezza privativa della libertà personale non inferiore a tre anni;
- g) «sistema di prenotazione», il sistema interno del vettore aereo in cui sono raccolti i dati PNR ai fini della gestione delle prenotazioni;
- h) «vettore aereo», l'impresa di trasporto aereo titolare di una licenza di esercizio in corso di validità o equivalente che le consente di effettuare trasporti aerei di passeggeri;
- i) «volo extra-UE», il volo di linea o non di linea effettuato da un vettore aereo proveniente da un Paese terzo e il cui atterraggio è previsto nel territorio nazionale oppure in partenza dal territorio nazionale e il cui atterraggio è previsto in



un Paese terzo, compresi, in entrambi i casi, i voli con scali nel territorio di Stati membri o di Paesi terzi;

l) «volo intra-UE», il volo di linea o non di linea effettuato da un vettore aereo proveniente dal territorio di uno Stato membro e il cui atterraggio è previsto nel territorio nazionale o viceversa, senza alcuno scalo nel territorio di un Paese terzo.

2. Ai fini del presente decreto si intendono, altresì, per:

a) «autorità competenti», le autorità responsabili della prevenzione e del perseguimento dei reati di terrorismo e dei reati gravi, individuate da ogni Stato membro e comunicate alla Commissione europea in conformità alla direttiva (UE) 2016/681;

b) «autorità competenti nazionali», le Forze di polizia di cui all'articolo 16, primo comma, della legge 1° aprile 1981, n. 121, la Direzione Investigativa Antimafia, gli organismi previsti dagli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, nonché la Direzione Nazionale Antimafia e Antiterrorismo di cui all'articolo 103 del decreto legislativo 6 settembre 2011, n. 159 e le Autorità giudiziarie competenti a perseguire i reati di cui al comma 1, lettere e) e f);

c) «CED», il Centro elaborazione dati di cui all'articolo 8 della legge 1° aprile 1981, n. 121;

d) «code sharing», il trasporto di passeggeri operato da uno o più vettori aerei per conto di altri vettori aerei e regolato da apposita convenzione;

e) «Codice in materia di protezione dei dati personali», il decreto legislativo 30 giugno 2003, n. 196;

f) «Dipartimento della Pubblica Sicurezza», il Dipartimento della Pubblica Sicurezza, di cui all'articolo 4 della legge 1° aprile 1981, n. 121;

g) «Direzione Centrale della Polizia Criminale», la Direzione Centrale della Polizia Criminale del Dipartimento della Pubblica Sicurezza, di cui all'articolo 5, primo comma, lett. c), della legge n. 121 del 1981;

h) «Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere», la Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere del Dipartimento della Pubblica Sicurezza, di cui all'articolo 35 della legge 30 luglio 2002, n. 189;

i) «ENAC», l'Ente nazionale per l'aviazione civile, istituito con decreto legislativo 25 luglio 1997, n. 250;

j) «frequent flyer», i viaggiatori abituali;

k) «riscontro negativo», l'esito dell'attività di analisi dei dati PNR effettuata dall'UIP nazionale in base alla quale un passeggero non è sospettato di essere implicato in un reato di terrorismo o in reati gravi;

l) «riscontro positivo», l'individuazione di un passeggero sospettato di essere implicato in un reato di terrorismo o in reati gravi, all'esito dell'attività di analisi dei dati PNR effettuata dall'UIP nazionale;

m) «Sistema Informativo», il sistema informativo per l'uso dei dati PNR, istituito presso il Dipartimento della Pubblica Sicurezza, finalizzato alla raccolta, al trattamento e al trasferimento dei dati PNR.

n) «Unità d'informazione sui passeggeri (UIP)», autorità competente, in materia di prevenzione e repressione dei reati di terrorismo e dei reati gravi, individuata da ciascuno Stato membro ai sensi della Direttiva (UE) 2016/681;



- o) «Unità d'informazione sui passeggeri (UIP) nazionale», l'unità istituita presso il Ministero dell'Interno, Dipartimento della Pubblica Sicurezza, nell'ambito della Direzione Centrale della Polizia Criminale competente in materia di prevenzione e repressione dei reati di terrorismo e dei reati gravi.
3. Ai fini del presente decreto si intendono, inoltre, per:
- a) «controllo alla frontiera», il controllo, effettuato alla frontiera, secondo le modalità indicate dall'articolo 2 del regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio del 9 marzo 2016;
- b) Sistema informativo frontaliero *Border Control System* (BCS): il sistema informativo istituito presso il Ministero dell'interno, Dipartimento della pubblica sicurezza, Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere per la raccolta e il trattamento delle informazioni acquisite ai sensi della direttiva 2004/82/CE;
- c) «dati API», parte dei dati PNR, comprendenti il tipo, il numero, paese di rilascio e la data di scadenza del documento di viaggio utilizzato, la cittadinanza, il nome completo, sesso, la data e il luogo di nascita, il valico di frontiera di ingresso nel territorio italiano, la compagnia aerea, il numero del volo, la data di partenza e di arrivo, l'ora di partenza, l'ora di arrivo e la durata del volo, l'aeroporto di partenza e di arrivo, il numero complessivo dei passeggeri trasportati con tale volo, il primo punto di imbarco;
- d) «frontiere esterne», le frontiere esterne dello Stato italiano con i Paesi non appartenenti all'Unione europea;
- e) «Uffici incaricati dei controlli di polizia di frontiera», gli uffici o reparti delle Forze di polizia incaricati dei controlli di polizia di frontiera;
- f) «valico di frontiera», il valico di frontiera presidiato da uffici o reparti delle Forze di polizia incaricati dei controlli di polizia di frontiera.

## CAPO II

### *Finalità del trattamento dei dati e organizzazione del Sistema Informativo*

#### ART. 3

##### *(Finalità dei trattamenti)*

1. I dati PNR raccolti a norma del presente decreto sono trattati a fini di prevenzione e repressione dei reati di terrorismo e dei reati gravi, secondo quanto previsto all'articolo 6, comma 2, lettere b), c) e d).
2. I dati API raccolti e resi disponibili agli Uffici incaricati dei controlli di polizia di frontiera a norma del presente decreto sono trattati al fine di migliorare i controlli alle frontiere esterne e prevenire l'immigrazione illegale. In caso di ripristino temporaneo dei controlli di frontiera alle frontiere interne il trattamento dei dati API è esteso anche ai voli *intra-UE*.



**ART. 4**  
*(Sistema Informativo)*

1. Ai fini della raccolta, del trattamento e del trasferimento dei dati PNR e dei dati API è istituito un apposito Sistema Informativo presso il Dipartimento della Pubblica Sicurezza che ne garantisce la gestione tecnica e informatica. A tal fine, il predetto Dipartimento è il titolare del trattamento dei dati PNR e dei dati API, secondo quanto previsto dal Codice in materia di protezione dei dati personali.
2. I responsabili del trattamento dei dati, secondo quanto previsto dal Codice in materia di protezione dei dati personali, sono la Direzione Centrale della Polizia Criminale per il trattamento dei dati e per le finalità previste dall'articolo 3, comma 1, e la Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere per il trattamento dei dati e per le finalità previste dall'articolo 3, comma 2.
3. Le interrogazioni del Sistema Informativo possono essere effettuate per le finalità di cui all'articolo 3; a ciascuna delle predette finalità corrisponde uno specifico profilo di autorizzazione.
4. Il trattamento dei dati PNR e dei dati API è consentito unicamente al personale cui siano state preventivamente rilasciate le necessarie credenziali di autenticazione.
5. Con uno o più decreti adottati, entro tre mesi dalla data di entrata in vigore del presente decreto, dal Ministro dell'interno, sentito il Garante per la protezione dei dati personali, sono disciplinate le modalità tecniche:
  - a) di funzionamento del Sistema Informativo;
  - b) di autenticazione, autorizzazione e registrazione degli accessi e delle operazioni effettuate nel Sistema Informativo;
  - c) di consultazione da parte dei soggetti autorizzati, ivi comprese le procedure tecniche e operative di mascheramento e cancellazione dei dati ai sensi dell'articolo 10;
  - d) di raffronto informatico dei dati PNR con quelli conservati nel CED e nelle altre banche dati nazionali, europee ed internazionali contenenti informazioni utili ai fini di prevenzione e repressione dei reati di terrorismo e dei reati gravi;
  - e) di raffronto informatico dei dati API con quelli conservati nel CED e nelle altre banche dati nazionali, europee ed internazionali contenenti informazioni utili ai fini di prevenzione dell'immigrazione irregolare;
  - f) di trasferimento delle informazioni, con strumenti informatici, dall'UIP nazionale alle autorità competenti nazionali;
  - g) di trasferimento dei dati PNR da parte dei vettori aerei.
6. Relativamente agli organismi previsti dagli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, le modalità di cui al comma 5, lettera f), sono disciplinate con un regolamento adottato, entro tre mesi dalla data di entrata in vigore del presente decreto, ai sensi degli articoli 13, comma 2, e 43 della legge n. 124 del 2007, di concerto con il Ministro dell'interno.
7. Il Sistema Informativo utilizza i formati di dati e i protocolli informatici comuni individuati con la decisione di esecuzione 2017/759/UE della Commissione, del 28 aprile 2017, garantisce l'individuazione del soggetto che effettua ciascuna interrogazione e conserva la traccia di ciascun accesso.
8. I vettori aerei che non effettuano voli *extra-UE* e *intra-UE* secondo un programma operativo pubblico specifico e che non possiedono l'infrastruttura necessaria



a supportare i formati di dati e i protocolli di trasmissione elencati nell'allegato della decisione di esecuzione di cui al comma 7 trasferiscono i dati PNR con un mezzo elettronico che offra adeguate garanzie rispetto alle misure di sicurezza tecniche, individuato dall'UIP nazionale con apposita prescrizione.

#### ART. 5

*(Modalità di trasferimento dei dati PNR al Sistema Informativo)*

1. I vettori aerei trasferiscono al Sistema Informativo, attraverso il «metodo *push*», i dati PNR relativi ai voli *extra-UE* e *intra-UE*, in partenza, in arrivo o facenti scalo nel territorio nazionale, raccolti nel normale svolgimento della loro attività. Per i voli operati in *code-sharing* da uno o più vettori aerei, il trasferimento dei dati PNR è effettuato dal vettore aereo che opera il volo.
2. Il trasferimento dei dati PNR è effettuato elettronicamente, utilizzando i formati di dati e i protocolli informatici di cui all'articolo 4, comma 7. I vettori aerei hanno l'obbligo di scegliere e notificare all'UIP nazionale il formato di dati e il protocollo informatico che intendono utilizzare per l'effettuazione dei trasferimenti. In caso di guasto tecnico, i dati PNR possono essere trasferiti con altro mezzo appropriato, che assicuri equivalenti livelli di sicurezza e sia conforme alle disposizioni vigenti in materia di protezione dei dati personali.
3. Il vettore, nel caso in cui debba procedere all'adeguamento dei propri sistemi informatici ai formati di dati e ai protocolli informatici di cui all'articolo 4, comma 7, nelle more di tale adeguamento, effettua il trasferimento dei dati PNR con un mezzo elettronico che offra sufficienti garanzie rispetto alle misure di sicurezza tecniche e alle misure organizzative relative ai trattamenti da effettuare.
4. I vettori aerei trasferiscono i dati PNR:
  - a) in un periodo compreso tra le ventiquattro e le quarantotto ore antecedenti all'orario previsto per la partenza del volo; e
  - b) immediatamente dopo la chiusura del volo, quando non è più possibile l'imbarco o lo sbarco di passeggeri, anche mediante l'aggiornamento dei dati trasferiti ai sensi della lettera a).
5. Nel caso di pericolo imminente e concreto che possa essere commesso un reato di terrorismo o un altro reato grave, i vettori aerei, su richiesta dell'UIP, trasferiscono senza ritardo i dati PNR anche in un momento antecedente a quelli indicati al comma 4.
6. Nel caso in cui i vettori trasferiscano dati diversi da quelli indicati nell'allegato I della direttiva (UE) 2016/681, l'UIP nazionale provvede senza ritardo alla loro definitiva cancellazione.

#### ART. 6

*(Unità d'informazione sui passeggeri (UIP) nazionale)*

1. L'UIP nazionale è composta da personale delle Forze di polizia di cui all'articolo 16, primo comma, della legge n. 121 del 1981. L'organizzazione dell'UIP nazionale e la relativa pianta organica sono definite con decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze, ai sensi dell'articolo 5, settimo comma, della legge n. 121 del 1981. Il relativo contingente di personale è determinato, ai sensi dell'articolo 6, secondo comma, della legge n. 121 del 1981, rispettivamente, con



decreto del Ministro dell'interno, con riguardo al personale appartenente ai ruoli della Polizia di Stato, e con decreto del Presidente del Consiglio dei Ministri, con riguardo al personale delle altre Forze di polizia.

2. L'UIP nazionale:

a) riceve, anche avvalendosi di un operatore economico qualificato, i dati PNR dai vettori aerei;

b) effettua, prima dell'arrivo o della partenza del volo, attività di analisi dei dati ricevuti al fine di individuare i passeggeri sospettati di essere implicati in reati di terrorismo o in reati gravi per i quali è necessario procedere a ulteriori verifiche da parte delle autorità competenti e di Europol;

c) sulla base di una richiesta debitamente motivata, provvede a comunicare, caso per caso, alle autorità competenti nazionali o, nei casi di cui all'articolo 14, alle autorità competenti di Stati membri ovvero, nelle ipotesi di cui all'articolo 18, a Europol i dati PNR o i risultati del loro trattamento;

d) all'esito dell'analisi dei dati PNR, aggiorna i criteri di cui all'articolo 8, comma 1, lettera b), sulla base dei quali sono effettuate le valutazioni finalizzate a individuare i passeggeri sospettati di essere implicati in reati di terrorismo o in reati gravi ai sensi della lettera b) del presente comma.

e) scambia sia i dati PNR che i risultati del loro trattamento con le UIP di altri Stati membri in conformità a quanto stabilito dagli articoli 13, 15, e 17.

#### ART. 7

*(Uffici incaricati dei controlli di polizia di frontiera)*

1. Gli Uffici incaricati di effettuare i controlli delle persone alle frontiere esterne attraverso le quali i passeggeri entrano nel territorio dello Stato provvedono al trattamento dei dati API per agevolare l'esecuzione di tali controlli al fine di prevenire l'immigrazione irregolare.

#### ART. 8

*(Trattamento dei dati PNR)*

1. Ai fini delle attività di analisi di cui all'articolo 6, comma 2, lettera b), l'UIP nazionale può:

a) confrontare i dati PNR con le informazioni contenute nel CED e nelle altre banche dati nazionali, europee ed internazionali contenenti informazioni utili ai fini di prevenzione e repressione dei reati di terrorismo e dei reati gravi;

b) trattare i dati PNR sulla base di criteri predeterminati ai sensi del comma 2.

2. I criteri di cui al comma 1, lettera b), sono individuati dall'UIP nazionale e periodicamente aggiornati sentite le autorità competenti nazionali, nel rispetto dei principi di proporzionalità, specificità e del divieto di discriminazione basata sull'origine razziale o etnica, sulle opinioni politiche, sulla religione o sulle convinzioni filosofiche, sull'appartenenza sindacale, sullo stato di salute, sulla vita sessuale o sull'orientamento sessuale dell'interessato.

3. L'UIP nazionale effettua le attività di analisi con modalità non discriminatorie.

4. I riscontri positivi risultanti dal trattamento automatizzato dei dati PNR, effettuato a norma dell'articolo 6 comma 2, lettera b), sono sottoposti dall'UIP



nazionale a un esame non automatizzato, condotto sul singolo caso, per verificare la necessità dell'adozione di provvedimenti e misure da parte delle autorità competenti nazionali, in conformità alle disposizioni vigenti.

5. I provvedimenti e le misure adottate ai sensi del comma 4 non pregiudicano il diritto di entrare nel territorio dello Stato delle persone che godono del diritto di libera circolazione all'interno dell'Unione europea in conformità al decreto legislativo 6 febbraio 2007, n. 30, e al regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio, del 9 marzo 2016.

#### ART. 9

##### *(Trattamento dei dati API)*

1. I dati API sono resi disponibili, attraverso il Sistema Informativo, agli Uffici incaricati dei controlli di polizia di frontiera, per le finalità di cui all'articolo 7, immediatamente dopo la chiusura del volo, quando non è più possibile l'imbarco o lo sbarco di passeggeri.

2. Entro ventiquattro ore dal momento della loro comunicazione agli Uffici di cui al comma 1, ovvero dopo l'ingresso dei passeggeri nel territorio dello Stato, i dati API non necessari per la prevenzione dell'immigrazione irregolare sono resi non visibili ai medesimi Uffici.

3. Per le finalità di cui all'articolo 3, comma 2, i dati API, trascorsi sei mesi dal loro ricevimento, sono resi indisponibili agli Uffici incaricati dei controlli di polizia di frontiera.

#### ART. 10

##### *(Periodo di conservazione dei dati PNR e trasformazione in forma anonima)*

1. I dati PNR trasmessi dai vettori aerei all'UIP nazionale sono conservati nel Sistema Informativo per un periodo di cinque anni dal loro trasferimento.

2. Dopo sei mesi dal loro trasferimento, i dati sono resi anonimi mediante mascheramento dei seguenti elementi:

- a) i nominativi di tutti i passeggeri figuranti nei dati PNR;
- b) il numero dei passeggeri figuranti nei dati PNR;
- c) l'indirizzo e le altre informazioni idonee a contattare i passeggeri;
- d) le informazioni sulle modalità di pagamento, compreso l'indirizzo di fatturazione, nel caso in cui esso contenga informazioni idonee ad identificare il passeggero cui si riferiscono i dati PNR o qualsiasi altra persona;
- e) le informazioni sui *frequent flyer*;
- f) le dichiarazioni di carattere generale contenenti informazioni idonee a consentire l'identificazione del passeggero cui si riferiscono i dati PNR;
- g) i dati API raccolti.

3. Allo scadere del periodo di sei mesi di cui al comma 2, la comunicazione dei dati PNR integrali è consentita solo se è necessaria per corrispondere a una richiesta formulata ai sensi dell'articolo 6, comma 2, lettera c), previa autorizzazione:



a) dell'Autorità giudiziaria, nel caso in cui la richiesta sia formulata nell'ambito di un procedimento penale o per l'applicazione di una delle misure di prevenzione di cui al Libro I, Titolo I, Capo II e Titolo II, Capo I del decreto legislativo 6 settembre 2011, n. 159; o

b) del Vice Capo della Polizia - Direttore Centrale della Polizia Criminale, per le finalità di prevenzione dei reati di terrorismo e dei reati gravi.

4. L'autorizzazione rilasciata ai sensi del comma 3 è comunicata al responsabile della protezione dei dati personali di cui all'articolo 21 per le verifiche di competenza.

5. I dati PNR sono cancellati in via definitiva allo scadere del periodo di cinque anni di cui al comma 1, secondo le modalità stabilite con uno dei decreti del Ministro dell'interno di cui all'articolo 4, comma 5. L'obbligo di cancellazione non si applica ai dati PNR trasferiti a una delle autorità competenti nazionali e utilizzati nell'ambito di un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi. In tali casi i dati PNR sono conservati nel rispetto delle disposizioni del codice di procedura penale o di quelle riguardanti i trattamenti per finalità di polizia, ovvero di quelle riguardanti i trattamenti effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

6. I risultati del trattamento di cui all'articolo 6, comma 2, lettera b), sono conservati per il tempo strettamente necessario a comunicare gli esiti di eventuali riscontri positivi alle autorità competenti nazionali ovvero alle UIP di altri Stati membri secondo le modalità stabilite dall'articolo 13, comma 1. I risultati dei trattamenti automatizzati, anche in caso di riscontro negativo all'esito di esame non automatizzato condotto sul singolo caso, sono conservati per un periodo non superiore a quello previsto dal comma 5, al fine di assicurare l'esattezza dei futuri riscontri.

7. I dati PNR e i dati API riversati, sulla base delle vigenti disposizioni, nel CED sono sottoposti alla specifica disciplina prevista per il medesimo CED.

#### **ART. 11**

*(Conservazione dei dati API)*

1. Il vettore aereo è obbligato a cancellare, entro ventiquattro ore dall'arrivo del volo, i dati API trasmessi.

### **CAPO III**

*Trasferimento e scambio dei dati PNR e dei risultati del loro trattamento*

#### **ART. 12**

*(Trasferimento dei dati PNR alle autorità competenti nazionali)*

1. L'UIP nazionale trasmette i dati PNR o i risultati del loro trattamento relativi ai passeggeri individuati ai sensi dell'articolo 6, comma 2, lettera b), a seguito dell'esame individuale non automatizzato, alle autorità competenti nazionali perché li sottopongano a ulteriore trattamento e adottino provvedimenti idonei a prevenire e reprimere reati di terrorismo o reati gravi. Per le medesime finalità, le autorità competenti nazionali



possono chiedere all'UIP nazionale la trasmissione dei dati PNR o dei risultati del loro trattamento. Tale trasmissione avviene con strumenti informatici, secondo le modalità stabilite con i decreti di cui all'articolo 4, comma 5, lettera e).

2. Le decisioni delle autorità competenti nazionali che determinino conseguenze giuridiche negative per l'interessato non possono essere adottate esclusivamente sulla base del trattamento automatizzato dei dati PNR, né possono fondarsi sull'origine razziale o etnica, sulle opinioni politiche, sulla religione o sulle convinzioni filosofiche, sull'appartenenza sindacale, sullo stato di salute, sulla vita sessuale o sull'orientamento sessuale dell'interessato.

#### **ART. 13**

*(Trasferimento dei dati PNR alle UIP degli Stati membri)*

1. Nel caso di riscontro positivo, l'UIP nazionale trasmette i dati PNR pertinenti e necessari o i risultati del loro trattamento alle UIP di altri Stati membri.

2. I dati PNR e i risultati del loro trattamento, se già effettuato, sono trasferiti all'UIP di altro Stato membro sulla base di una richiesta, riguardante anche solo una parte dei dati PNR, debitamente motivata in relazione a un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi. L'UIP nazionale comunica le predette informazioni senza ritardo.

3. Nel caso in cui i dati richiesti siano stati resi anonimi a norma dell'articolo 10, comma 2, l'UIP nazionale trasmette all'UIP di altro Stato membro i dati PNR integrali solo se necessario per corrispondere a una richiesta formulata ai sensi dell'articolo 6, comma 2, lettera c), previa autorizzazione delle autorità di cui all'articolo 10, comma 3.

4. Nel caso di pericolo imminente e concreto che possa essere commesso un reato di terrorismo o un altro reato grave, l'UIP di uno Stato membro può chiedere all'UIP nazionale che i dati PNR siano trasmessi, ai sensi dell'articolo 5, comma 5, anche in un momento antecedente a quelli indicati dall'articolo 5, comma 4.

#### **ART. 14**

*(Trasferimento dei dati PNR alle autorità competenti degli Stati membri)*

1. L'UIP nazionale trasmette i dati PNR direttamente alle autorità competenti di altri Stati membri che ne abbiano fatto richiesta, nel rispetto delle previsioni recate dall'articolo 13, commi 2 e 3, in presenza di situazioni di emergenza che non consentano di inoltrare la medesima richiesta attraverso l'UIP del proprio Stato.

#### **ART. 15**

*(Trasferimento dei dati PNR da parte di Stati membri)*

1. L'UIP nazionale può chiedere all'UIP di altro Stato membro la trasmissione dei dati PNR, nonché dei risultati del loro trattamento. Tale richiesta, riguardante anche solo una parte dei dati PNR, deve essere debitamente motivata in relazione a un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi. L'UIP nazionale trasmette le informazioni ricevute alle autorità competenti nazionali, ai sensi dell'articolo 12, comma 1.



2. Nel caso di pericolo imminente e concreto che possa essere commesso un reato di terrorismo o altro reato grave, l'UIP nazionale può chiedere all'UIP di altro Stato membro che i dati PNR siano trasmessi, ai sensi dell'articolo 5, comma 5, anche in un momento antecedente a quelli indicati dall'articolo 5, comma 4.

#### **ART. 16**

*(Richiesta dei dati PNR da parte delle autorità competenti nazionali)*

1. Le autorità competenti nazionali inoltrano le richieste di dati PNR alle UIP degli altri Stati membri tramite l'UIP nazionale.
2. In situazioni di emergenza che non consentano di inoltrare la richiesta attraverso l'UIP nazionale, le autorità competenti nazionali possono richiedere direttamente all'UIP di altro Stato membro la trasmissione dei dati PNR, nel rispetto delle previsioni recate dall'articolo 13, comma 2. Copia della richiesta è inoltrata tempestivamente all'UIP nazionale.

#### **ART. 17**

*(Modalità di scambio delle informazioni)*

1. Lo scambio di informazioni ai sensi degli articoli 13, 14, 15 e 16 può avvenire tramite qualsiasi canale esistente di cooperazione internazionale di polizia. La lingua utilizzata per la richiesta e lo scambio di informazioni è quella applicabile al canale utilizzato.
2. In casi di emergenza, il punto di contatto nazionale è l'UIP nazionale.

#### **ART. 18**

*(Trasferimento dei dati PNR a Europol)*

1. Europol può richiedere, entro i limiti delle proprie competenze e per l'adempimento dei propri compiti, i dati PNR o i risultati del loro trattamento all'UIP nazionale quando strettamente necessario per sostenere e rafforzare l'azione degli Stati membri volta alla prevenzione e alla repressione di uno specifico reato di terrorismo o altro reato grave, a condizione che si tratti di un reato di propria competenza ai sensi del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio dell'11 maggio 2016.
2. La richiesta è formulata attraverso sistemi informatici, utilizzando l'applicazione SIENA, per il tramite dell'Unità Nazionale Europol e deve contenere i motivi per i quali Europol ritiene necessaria la trasmissione dei dati PNR o dei risultati del loro trattamento ai fini di prevenzione e repressione dei reati di terrorismo o dei reati gravi di propria competenza.
3. L'UIP trasmette le informazioni ai sensi del presente articolo attraverso l'applicazione SIENA secondo le disposizioni di cui al regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016. La lingua utilizzata per la richiesta e lo scambio di informazioni è quella applicabile a SIENA.



## ART. 19

### *(Trasferimento dei dati PNR a paesi terzi)*

1. Fatte salve le condizioni previste da eventuali accordi internazionali, i dati PNR e i risultati del loro trattamento possono essere trasferiti alle autorità competenti di un Paese terzo in relazione a casi individuali, soltanto in conformità alle previsioni del presente decreto e alle disposizioni del Codice per la protezione dei dati personali concernenti il trasferimento verso Paesi terzi di dati giudiziari o trattati per finalità di polizia e qualora ricorrano le seguenti condizioni:

a) la richiesta sia formulata nel rispetto delle previsioni recate dall'articolo 13, commi 2 e 3;

b) il trasferimento sia necessario per le finalità di cui all'articolo 3, comma 1;

c) il Paese terzo si impegni a trattare i dati con le garanzie previste dal presente decreto e a ritrasferire i dati a altro Paese terzo soltanto per le finalità di cui all'articolo 3, comma 1, e previa autorizzazione espressa dello Stato italiano.

2. Fermo restando quanto previsto al comma 1, i dati PNR possono essere trasferiti senza il previo consenso dello Stato membro dal quale sono stati ottenuti nel caso in cui ricorrano contestualmente le seguenti condizioni:

a) il trasferimento sia indispensabile per rispondere a una minaccia specifica e reale connessa a reati di terrorismo o a reati gravi in uno Stato membro o in un Paese terzo;

b) il consenso preliminare non possa essere ottenuto in tempo utile.

3. Il trasferimento dei dati senza il preventivo consenso è comunicato all'UIP dello Stato che ha trasmesso il dato. Il trasferimento è annotato in apposito registro per le verifiche da parte del responsabile della protezione dei dati.

## CAPO IV

### *Disposizioni in materia di protezione dei dati personali*

## ART. 20

### *(Autorità nazionale di controllo)*

1. L'Autorità nazionale di controllo è il Garante per la protezione dei dati personali, che esercita il controllo sul trattamento dei dati personali effettuato in applicazione del presente decreto, con le modalità previste dal Codice in materia di protezione dei dati personali.

2. La medesima autorità, su richiesta dell'interessato, esprime pareri in merito all'esercizio dei diritti di protezione dei dati personali derivanti dalle disposizioni del presente decreto.



## ART. 21

*(Responsabile della protezione dei dati)*

1. Il responsabile della protezione dei dati è nominato con decreto del Capo della Polizia – Direttore Generale della Pubblica Sicurezza, nell'ambito della Direzione Centrale della Polizia Criminale e adempie alle proprie funzioni in modo indipendente.
2. Il responsabile della protezione dei dati è incaricato di vigilare sul corretto trattamento dei dati PNR e garantisce l'attuazione di tutte le misure tecniche e di sicurezza, nel rispetto di quanto disposto dal Codice per la protezione dei dati personali.
3. Il responsabile della protezione dei dati è il punto di contatto unico per gli interessati, in merito a tutte le questioni connesse al trattamento dei dati PNR che li riguardano.
4. Il responsabile della protezione dei dati ha accesso ai dati trattati dall'UIP nazionale e segnala al Garante per la protezione dei dati personali i casi in cui il trattamento dei dati non sia stato effettuato lecitamente.

## ART. 22

*(Protezione dei dati personali)*

1. In relazione al trattamento dei dati personali effettuato ai sensi del presente decreto si applicano le disposizioni del Codice per la protezione dei dati personali di cui alla Parte II, Titolo II, Capo I, e Titolo III, limitatamente ai trattamenti effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.
2. Al trattamento di dati effettuato ai sensi del presente decreto si applicano le disposizioni di cui agli articoli da 33 a 36 del Codice per la protezione dei dati personali.
3. Al trattamento di dati personali da parte dei vettori aerei si applicano le disposizioni del Codice per la protezione dei dati personali, anche per quanto concerne l'obbligo di informare adeguatamente i passeggeri e di adottare adeguate misure tecniche e organizzative a tutela della sicurezza e della riservatezza dei dati personali.
4. E' vietato il trattamento dei dati PNR idoneo a rivelare l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale, lo stato di salute, la vita o l'orientamento sessuale dell'interessato.
5. L'UIP nazionale cancella immediatamente i dati PNR trattati con modalità tali da rivelare le informazioni di cui al comma precedente.
6. L'UIP nazionale adotta adeguate misure e procedure tecniche e organizzative per garantire un livello elevato di sicurezza in relazione ai rischi connessi al trattamento dei dati PNR anche nelle ipotesi di cui all'articolo 5, commi 2 e 3. L'UIP nazionale conserva la documentazione relativa ai sistemi e alle procedure di trattamento. La predetta documentazione riporta l'indicazione dei seguenti dati:
  - a) l'organizzazione dell'UIP nazionale e gli indirizzi utili a contattare le sue articolazioni interne;
  - b) i nominativi e gli indirizzi del personale dell'UIP nazionale incaricato del trattamento dei dati PNR;
  - c) il registro dei livelli di autorizzazione all'accesso di cui è titolare il personale dell'UIP nazionale;
  - d) le richieste formulate dalle autorità competenti nazionali;



- e) le richieste formulate dalle UIP e dalle autorità competenti di altri Stati membri;
- f) le richieste formulate da Paesi terzi e i trasferimenti di dati effettuati.

7. L'UIP nazionale conserva, altresì, per un periodo di cinque anni, i registri delle attività di raccolta, consultazione, comunicazione e cancellazione dei dati. Detti registri riportano l'indicazione della finalità, della data e dell'ora dell'operazione e gli elementi relativi all'identità della persona che ha consultato o comunicato i dati PNR, nonché dei destinatari di tali dati. I registri sono usati esclusivamente a fini di verifica, di autocontrollo, per garantire l'integrità e la sicurezza dei dati o di audit.

8. La documentazione di cui al comma 6 e i registri di cui al comma 7 sono messi a disposizione del Garante per la protezione dei dati personali, a seguito di richiesta.

9. In caso di violazione di dati personali, l'UIP nazionale ne dà comunicazione senza ritardo al Garante per la protezione dei dati personali. Quando tale violazione rischia di arrecare un rilevante pregiudizio ai dati personali o alla riservatezza dell'interessato, l'UIP nazionale comunica senza indebito ritardo all'interessato e al Garante per la protezione dei dati personali l'avvenuta violazione.

#### ART. 23

##### *(Diritti dell'interessato)*

1. In relazione ai trattamenti di dati personali effettuati in applicazione del presente decreto, sono riconosciuti all'interessato i diritti di cui all'articolo 10, commi 3, 4 e 5, della legge n. 121 del 1981. Tali diritti sono esercitati con istanza rivolta alla Direzione Centrale della Polizia Criminale, con la quale l'interessato può domandare, altresì, che sia data evidenza dell'esercizio dei diritti di cui al presente articolo nel Sistema Informativo.

2. La Direzione Centrale della Polizia Criminale comunica all'interessato i provvedimenti adottati a seguito delle richieste formulate ai sensi del comma 1.

3. Il responsabile della protezione dei dati, l'UIP nazionale e l'UIP dello Stato membro eventualmente interessato sono informati della presentazione dell'istanza di cui al comma 1.

4. L'indicazione di cui al comma 1, secondo periodo, può essere rimossa a richiesta dell'interessato o su provvedimento del Garante per la protezione dei dati personali o dell'Autorità giudiziaria, adottati ai sensi del Codice per la protezione dei dati personali.

#### CAPO V

##### *Disposizioni sanzionatorie e finali*

#### ART. 24

##### *(Sanzioni)*

1. Salvo che il fatto costituisca reato, il vettore che non trasmette i dati, ovvero li trasmette in modo difforme da quanto previsto dall'articolo 5, è punito con la sanzione amministrativa pecuniaria da euro 10.000 ad euro 100.000 per ogni viaggio a cui si riferisce la condotta. La medesima sanzione amministrativa pecuniaria si applica in caso



di trasmissione di dati incompleti o errati. La sanzione di cui al primo periodo si applica, altresì, al vettore aereo che non adempia entro il termine fissato alle prescrizioni dell'UIP nazionale, adottate per garantire il trasferimento dei dati PNR al Sistema Informativo.

2. L'autorità competente a irrogare le sanzioni di cui al comma 1 è l'ENAC, cui è trasmesso il rapporto previsto dall'articolo 17 della legge 24 novembre 1981, n. 689.

3. Nei casi in cui le violazioni di cui al comma 1 siano commesse con la condizione della reiterazione di cui all'articolo 8-bis della legge n. 689 del 1981, l'ENAC può disporre la sospensione da uno a dodici mesi, ovvero la revoca della licenza, autorizzazione o concessione rilasciata dall'autorità amministrativa italiana, inerente all'attività professionale svolta e al mezzo di trasporto utilizzato.

4. La violazione dell'obbligo di cancellazione dei dati API previsto dall'articolo 11 è punito con la sanzione amministrativa pecuniaria da euro 5.000 ad euro 50.000. L'autorità competente a irrogare la sanzione è il Garante per la protezione dei dati personali, ai sensi dell'articolo 166 del Codice per la protezione dei dati personali.

5. Resta ferma l'applicazione dell'articolo 12, comma 6, del Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286.

#### **ART. 25**

*(Statistiche)*

1. Il Ministero dell'interno comunica, annualmente, alla Commissione europea elaborazioni statistiche concernenti i dati PNR trasmessi all'UIP nazionale. Tali elaborazioni non contengono dati personali e comprendono:

- a) il numero totale di passeggeri i cui dati PNR sono stati raccolti e scambiati;
- b) il numero di passeggeri individuati a fini di ulteriori verifiche ai sensi dell'articolo 6, comma 2, lettera b).

#### **ART. 26**

*(Disposizioni transitorie e finali)*

1. Le disposizioni di cui al decreto legislativo 2 agosto 2007, n. 144, continuano ad applicarsi fino alla data di entrata in vigore dell'ultimo dei provvedimenti di attuazione di cui agli articoli 4, commi 5 e 6, 6, comma 1, e 10, comma 5. Dalla medesima data il decreto legislativo n. 144 del 2007 è abrogato.

2. I riferimenti ovunque presenti al Sistema informativo frontaliere BCS si intendono sostituiti dai riferimenti al Sistema Informativo di cui all'articolo 4.



**ART. 27**

*(Clausola di neutralità finanziaria)*

1. Dall'attuazione delle disposizioni del presente decreto non devono derivare nuovi o maggiori oneri per la finanza pubblica. Le Amministrazioni interessate provvedono ai conseguenti adempimenti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Il presente decreto, munito del sigillo di Stato, sarà inserito nella Raccolta Ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

