SENATO DELLA REPUBBLICA

XVII LEGISLATURA

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

(Parere ai sensi degli articoli 1 e 12 della legge 25 ottobre 2017, n. 163)

(Trasmesso alla Presidenza del Senato il 21 febbraio 2018)

La Ministra
per i rapporti con il Parlamento

DRP/II/XVII/D352/18

Roma, 21 febbraio 2018

Signor Presidente,

trasmetto, al fine dell'espressione del parere da parte delle competenti Commissioni parlamentari, lo 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, approvato in via preliminare dal Consiglio dei ministri l'8 febbraio 2018.

In considerazione dell'imminente scadenza della delega, Le segnalo, a nome del Governo, l'urgenza dell'esame del provvedimento da parte delle competenti Commissioni parlamentari pur se privo del parere del Garante per la protezione dei dati personali, che mi riservo di trasmettere non appena sarà acquisito.

Cordialmente,

Anna Finocchiaro

Sen. Pietro GRASSO
Presidente del Senato della Repubblica
ROMA

Relazione illustrativa

Il presente decreto legislativo attua nell'ordinamento interno le disposizioni della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (di seguito, «direttiva PNR»), ed è adottato dal Governo nell'esercizio della delega conferita dall'articolo 12 della legge 25 ottobre 2017, n. 163 - Legge di delegazione europea 2016-2017, pubblicata nella Gazzetta Ufficiale del 6 novembre 2017, n. 259.

La direttiva PNR si prefigge l'obiettivo di rafforzare il sistema di sicurezza europeo tramite mirati controlli sui flussi di passeggeri aerei all'interno e all'esterno dell'Unione europea.

Più in dettaglio, tali controlli si sviluppano attraverso l'analisi delle informazioni che ciascun passeggero fornisce ai vettori aerei in fase di prenotazione del volo. Si tratta di un insieme di dati particolarmente ampio che consente un'attività di analisi di assoluto rilievo, all'esito della quale possono essere individuati soggetti che non sono necessariamente già noti alle Autorità ma che, per le caratteristiche dei viaggi effettuati, appaiono meritevoli di ulteriori approfondimenti ai fini del terrorismo e delle altre gravi forme di criminalità.

Il decreto disciplina, contestualmente, l'obbligo di trasmissione delle informazioni introdotto dalla direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate (di seguito, «direttiva API»), assorbendo la relativa normativa di attuazione e disponendo l'abrogazione della stessa dal momento dell'entrata in vigore dei propri provvedimenti attuativi. In tal senso, si evidenzia che i dati API, riferiti ai viaggiatori effettivamente presenti a bordo degli aeromobili al momento dell'attraversamento della frontiera, costituiscono una porzione dei dati PNR, che comprendono anche quelli relativi ai soggetti iscritti nelle liste di imbarco, indipendentemente dal fatto che siano stati o meno trasportati.

Tenendo presente questa circostanza, si è ritenuto opportuno assorbire nello schema di provvedimento anche la regolamentazione del trattamento dei dati API. Ciò è, peraltro, conforme agli enunciati recati dalla direttiva (UE) 2016/681, a cominciare dai "considerando" nn. 9 e 10, dai quali si evince, in sintesi, che per la realizzazione del sistema di trattamento dei dati PNR, gli Stati membri devono assicurare la raccolta e la trasmissione da parte dei vettori dei medesimi dati PNR, *"compresi i dati API"*.

Tale processo di assorbimento risponde all'esigenza di soddisfare i principi direttivi della massima semplificazione dei procedimenti, delle modalità di organizzazione dei servizi e normativa, enunciato dall'articolo 32 della legge 24 dicembre 2012, n. 234, cui fa rinvio il predetto articolo 12 della legge di delegazione europea 2016-2017.

Ai sensi della direttiva API, i vettori aerei hanno l'obbligo di trasmettere agli Uffici incaricati di effettuare i controlli di polizia di frontiera determinate informazioni, sostanzialmente anagrafiche (di seguito, «dati API»), relative ai passeggeri trasportati su voli *extra*-UE che fanno ingresso nel territorio dello Stato. Tale onere di trasmissione deve essere adempiuto una volta terminata la procedura di imbarco, al fine di consentire ai predetti Uffici di eseguire un'analisi preventiva dei dati dei passeggeri (tramite l'interrogazione di determinate banche dati nazionali ed internazionali), in anticipo rispetto al momento dell'arrivo del volo e dell'arrivo dei viaggiatori presso il cd. *Border Crossing Point,* migliorando l'efficienza delle verifiche di frontiera e assicurando una più proficua azione di prevenzione dell'immigrazione irregolare.

Ai sensi della direttiva PNR, i vettori aerei hanno l'obbligo di trasmettere determinate informazioni, elencate dettagliatamente nell'allegato I (di seguito, «dati PNR»), concernenti i passeggeri di voli *extra*-UE e *intra*-UE, in ingresso e in uscita dal territorio dello Stato, all'Unità d'informazione sui passeggeri (di seguito, «UIP»), appositamente istituita e avente la funzione principale di individuare, attraverso l'analisi dei dati PNR, i passeggeri implicati in reati di terrorismo o in altri reati gravi.

Da tale sintetica descrizione del contenuto dei due Atti europei, si evince agevolmente la presenza di elementi comuni che appaiono giustificare la decisione di procedere ad una regolamentazione attuativa unitaria: l'identità dell'oggetto, ossia l'obbligo di trasmissione di informazioni relative ai passeggeri, e l'identità del soggetto su cui tale onere grava, ovvero i vettori aerei.

La scelta di assorbire nel presente provvedimento la disciplina dei dati API trova conforto nel fatto che le informazioni contenute in questi ultimi costituiscono una "parte" dei dati PNR. I dati API, infatti, sono un sottoinsieme dei dati PNR e, come tali, vengono trasferiti dai vettori assieme ai restanti dati contenuti nel codice di prenotazione. Pertanto, l'eventuale coesistenza di due normative nazionali autonome assoggetterebbe l'obbligo di trasmissione dei dati API a fonti normative diverse, dando vita a una situazione di incertezza. Ciò implicherebbe una duplicazione degli adempimenti per i vettori aerei, nonché l'istituzione di due diversi sistemi informativi contenenti dati personali parzialmente sovrapponibili.

La scelta di realizzare un "contenitore" unico, nell'ambito del quale raccogliere e trattare i dati API e i dati PNR, si rivela più coerente e conforme al "principio di necessità" sancito dall'articolo 3 del Codice per la protezione dei dati personali, ai sensi del quale i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi.

L'operazione di semplificazione e razionalizzazione in parola appare ragionevole anche in considerazione del principio ispiratore che sembra aver guidato l'elaborazione di entrambe le discipline comunitarie, ovvero l'introduzione di un meccanismo di condivisione delle informazioni che, seppure articolato in maniera

diversa per dati API e dati PNR, è comunque finalizzato al rafforzamento della tutela della sicurezza all'interno dello spazio comune europeo.

A ciò si aggiungono le precise indicazioni contenute in alcune specifiche disposizioni, e cioè:

- l'art. 8, paragrafo 2, che sancisce l'obbligo a carico degli Stati membri di adottare le misure necessarie per il trasferimento anche dei dati API, attraverso il cd. "metodo *push*" (trasferimento dei dati dal vettore all'Autorità), prevedendo che tutte le disposizioni della direttiva (UE) 2016/681 si applichino anche ai predetti dati API. La disposizione palesa l'intendimento di ammettere la possibilità di regolamentare in un contesto normativo unico le modalità di trasmissione delle due tipologie di informazioni in questione;
- l'art. 12, paragrafo 2 - concernente il "mascheramento", dopo sei mesi dal trasferimento, degli elementi contenuti nei dati PNR, capaci di consentire l'identificazione diretta del passeggero – prevede che tale misura trovi applicazione anche ai dati API. Ciò rafforza il convincimento che le due tipologie di informazioni presentino stretti punti di sovrapponibilità che ne giustificano l'assoggettamento ad una disciplina unitaria, purché in grado di assicurare modalità di trattamento differenziate in ragione delle diverse finalità previste per ciascuna delle predette categorie di informazioni. Si muove in tale ottica l'ulteriore considerazione che il periodo massimo di conservazione dei dati API indispensabili a prevenire pericoli per l'ordine pubblico, la sicurezza nazionale o per esigenze di indagine (art. 4, comma 2, del decreto legislativo n. 144 del 2007) coincide con il periodo in cui i dati PNR sono conservati "in chiaro" (appunto sei mesi dal loro trasferimento).
- l'Allegato I, concernente i dati PNR, elenca gli elementi costitutivi dei dati PNR, includendovi, al punto 18, i dati API.

La soluzione "unitaria" postulata dallo schema di provvedimento rappresenta un'evidente misura di semplificazione sia degli adempimenti a carico dei vettori – che non devono adempiere a due analoghi oneri di trasmissione – sia delle attività organizzative a carico dell'Amministrazione, che può giovarsi di un unico sistema - ad accessi selettivi in ragione delle diverse finalità di trattamento del dato - con chiari risparmi di spesa sul lungo periodo.

Da ultimo, giova ribadire che la soluzione di disciplinare in un contesto unico il trattamento dei dati PNR e API, con la previsione di un unico Sistema informativo, rappresenta l'opzione di maggior salvaguardia dei principi di necessità e non eccedenza in materia di protezione dei dati personali, sanciti dal Codice della *privacy* e ribaditi anche dalla direttiva (UE) 2016/680.

Ciò premesso, il provvedimento si compone di ventisette articoli, suddivisi in cinque Capi.

Il **Capo I** (articoli 1 e 2) contiene disposizioni di carattere generale.

Più in dettaglio, l'**articolo 1**, ai commi 1 e 2, enuncia l'obiettivo dell'intervento normativo, ossia l'attuazione della direttiva PNR con contestuale rimodulazione della disciplina della trasmissione e del trattamento dei dati API, alla luce di quanto rappresentato in premessa.

Tale disposizione, in ossequio al criterio direttivo di delega previsto dal citato articolo 12 della legge di delegazione europea 2016-2017, prevede l'avvalimento, da parte dello Stato italiano, della facoltà concessa dall'articolo 2 della normativa comunitaria, che facoltizza l'estensione dell'applicazione dell'obbligo di trasmissione dei dati PNR anche in relazione ai voli *intra*-UE.

Il comma 3 definisce l'ambito di applicazione, precisando che l'attuazione della direttiva non pregiudica 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 stessa, né l'applicazione degli obblighi derivanti da accordi bilaterali o multilaterali conclusi con Stati non appartenenti all'Unione europea.

L'**articolo 2** reca norme di carattere definitorio, anche ulteriori rispetto a quelle previste dalla direttiva PNR, tra le quali meritano di essere segnalate:

- il comma 1, lett. *a)*, che, riprendendo la definizione di codice di prenotazione prevista dall'articolo 3, par. 1, n. 5), della direttiva PNR, chiarisce il significato di "dati PNR" e rimanda, ai fini di una più precisa determinazione, all'allegato I della direttiva stessa;
- il comma 2, lett. *b)*, ai sensi del quale, per "autorità competenti nazionali" si intendono le Forze di polizia di cui all'articolo 16, primo comma, della legge 1 aprile 1981, n. 121, la Direzione Investigativa Antimafia, gli Organismi di informazione e sicurezza facenti parte del Sistema di Informazione per la Sicurezza della Repubblica, di cui agli articoli 4, 6 e 7 della Legge n. 124/2007, nonché la Direzione Nazionale Antimafia e Antiterrorismo e le Autorità giudiziarie competenti a perseguire i reati di cui al comma 1, lettere e) e f);
- il comma 2, lett. *m)*, che introduce la nozione di "Sistema informativo" quale strumento istituito *ex novo* per la raccolta, il trattamento e il trasferimento dai dati PNR. Si precisa che, essendo i dati API contenuti nei dati PNR, il Sistema informativo assicura anche il trattamento dei dati API;
- il comma 2, lett. *o)*, ai sensi del quale l'"Unità d'informazione sui passeggeri (UIP) nazionale" è l'unità a composizione interforze istituita al fine di trattare i dati PNR e adottare le misure necessarie a prevenire e reprimere reati di terrorismo o determinati altri reati gravi. L'UIP nazionale è incardinata presso il Dipartimento di pubblica sicurezza, in conformità al criterio di delega recato dall'articolo 12 della Legge di delegazione europea 2016-2017 e, nell'ambito di tale Dipartimento, presso la Direzione Centrale della Polizia Criminale, individuata come l'articolazione dipartimentale che, per le specifiche attribuzioni

e per la composizione interforze, risulta più idonea a accogliere un'unità con le caratteristiche e le funzioni dell'UIP nazionale;

- il comma 3, lett. *c)*, che definisce i dati API quali parte dei dati PNR, contenuti, alla stregua di tutti i dati PNR, nel codice di prenotazione e completa la definizione elencando dettagliatamente le singole informazioni componenti il quadro. Tale elenco è il risultato della combinazione tra l'originaria previsione della direttiva API (articolo 3), la conseguente relativa disciplina attuativa (articolo 3, comma 2, decreto legislativo 2 agosto 2007, n. 144) e la disposizione dell'Allegato I, n. 18 della direttiva PNR.

Il **Capo II** individua le specifiche finalità per le quali i dati PNR e i dati API possono essere trattati (articolo 3) e delinea l'organizzazione complessiva del sistema, definendo il funzionamento del Sistema informativo (articoli 4 e 5), i soggetti legittimati all'effettuazione del trattamento (articoli 6 e 7), le modalità operative del trattamento (articoli 8 e 9) e le condizioni per la conservazione dei dati (articoli 10).

L'**articolo 3** sancisce il principio della limitazione delle finalità, stabilendo che i dati PNR e i dati API possono essere trattati, rispettivamente, al fine di prevenire e reprimere reati di terrorismo o altri reati gravi e al fine di prevenire il fenomeno dell'immigrazione irregolare.

Inoltre, la disposizione prevede che in caso di ripristino temporaneo dei controlli di frontiera alle frontiere interne, la disciplina dettata dal presente decreto in materia di trattamento dei dati API si estende anche ai voli *intra*-UE.

L'**articolo 4** istituisce il Sistema informativo finalizzato alla raccolta e al trattamento dei dati PNR e dei dati API e ne detta le regole di utilizzo: le interrogazioni possono essere effettuate esclusivamente per le finalità di cui all'articolo 3 e unicamente da parte del personale titolare di uno specifico profilo di autorizzazione.

Inoltre, in conformità a quanto previsto dal Codice per la protezione dei dati personali, si attribuiscono le funzioni di titolare del trattamento dei dati PNR e dei dati API al Dipartimento della pubblica sicurezza e le funzioni di responsabile del trattamento a due diverse articolazioni del predetto Dipartimento e, più in dettaglio, alla Direzione centrale della polizia criminale con riferimento ai dati PNR e alla Direzione centrale dell'immigrazione e della polizia delle frontiere con riferimento ai dati API.

In relazione ai profili tecnici di funzionamento del Sistema informativo si rinvia a uno o più decreti ministeriali da adottarsi, entro tre mesi dalla data di entrata in vigore del decreto, dal Ministro dell'interno, sentito il Garante per la protezione dei dati personali.

Per le modalità di trasmissione delle informazioni dall'UIP nazionale agli organismi del "comparto *intelligence*" previsti dagli articoli 4, 6 e 7 della legge n. 124 del 2007, è

prevista l'adozione di un regolamento ai sensi degli articoli 13, comma 2, e 43 della medesima legge, di concerto con il Ministro dell'interno.

Viene inoltre prescritto l'obbligo per i vettori aerei di utilizzare, per la trasmissione dei dati, i formati di dati e i protocolli informatici individuati dalla Commissione europea con decisione di esecuzione n. 2017/759/UE della Commissione, del 28 aprile 2017. I vettori aerei che non effettuano voli secondo un programma operativo pubblico specifico e non possiedono l'infrastruttura necessaria a supportare gli anzidetti formati di dati e protocolli di trasmissione, in conformità a quanto previsto dall'articolo 1, paragrafo 3 della citata decisione, 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.

Si precisa, infine, che ai fini dell'istituzione del Sistema informativo, sarà realizzata apposita piattaforma informatica presso il Centro Elettronico Nazionale della Polizia di Stato di Napoli, con connessione al sito di *Disaster Recovery* (*Business Continuity*) presso il Centro Polifunzionale della Polizia di Stato di Bari.

L'**articolo 5** prescrive l'obbligo per i vettori aerei di trasferire al Sistema informativo i dati PNR relativi ai passeggeri di voli *extra*-UE e *intra*-UE, in partenza, in arrivo o facenti scalo nel territorio nazionale.

In particolare, la trasmissione deve avvenire attraverso il "metodo *push*" (modalità di comunicazione che, secondo il legislatore europeo, offre un elevato livello di protezione dei dati), con mezzo elettronico, utilizzando i formati di dati e i protocolli informatici stabiliti dalla Commissione europea con la citata decisione di esecuzione 2017/759/UE in un periodo compreso tra le ventiquattro e le quarantotto ore antecedenti all'orario previsto per la partenza del volo e immediatamente dopo la chiusura dello stesso. Tuttavia, se l'accesso ai dati PNR risulta necessario per affrontare un pericolo imminente e concreto che possa essere commesso un reato di terrorismo o un altro reato grave, le informazioni possono essere trasmesse anche in un momento precedente quelli appena indicati.

Viene definito anche l'oggetto dell'obbligo di trasmissione, sancendo il principio di tassatività dei dati PNR: i vettori aerei devono trasferire unicamente le informazioni indicate nell'allegato I della direttiva PNR. In caso di trasmissione di dati diversi, l'UIP nazionale provvede senza ritardo alla loro definitiva cancellazione.

Nella disposizione in esame confluisce la disciplina dell'obbligo dei vettori aerei di trasmettere i dati API e la motivazione è di tutta evidenza: i dati API, essendo un sottoinsieme dei dati PNR, vengono trasmessi al Sistema informativo contestualmente agli altri dati contenuti nel codice di prenotazione.

L'**articolo 6** si occupa della composizione e delle funzioni dell'UIP nazionale, l'organo che si pone in posizione di assoluta centralità nel complesso sistema di introdotto nel nostro ordinamento ai fini dell'attuazione della direttiva PNR.

L'UIP nazionale, infatti, è incaricata di effettuare l'operazione principe, ossia l'attività di analisi dei dati PNR trasmessi dai vettori aerei, al fine di individuare i passeggeri che potrebbero essere implicati in reati di terrorismo o in altri reati gravi. Per di più, in caso di riscontro positivo, ossia qualora il sospetto su uno o più passeggeri risulti fondato, l'UIP nazionale trasmette le informazioni alle autorità competenti nazionali o alle omologhe UIP estere, esercitando una funzione propulsiva rispetto allo strutturato meccanismo di circolarità delle informazioni disciplinato dal successivo Capo III.

Al riguardo, si precisa che il recepimento della direttiva implica l'afflusso di informazioni riguardanti oltre 200.000.000 di passeggeri. Tale rilevante mole di dati può richiedere, soprattutto nella fase di prima attuazione, la necessità di fare ricorso all'intervento di operatori economici in possesso del necessario *know how* ai fini della loro acquisizione, mediante adeguati *software*. L'articolo 6, comma 2, lett. a), disciplinando questa eventualità, mira a garantire – senza aggravi per i vettori, ma comunque nel rispetto della clausola di invarianza finanziaria, che presidia l'intero provvedimento - l'acquisizione centralizzata dei dati da parte dell'UIP e il loro riversamento al Sistema informativo.

Inoltre, trattandosi dell'attore che, in via principale e prevalente, dispone delle informazioni sui passeggeri e ne effettua il trattamento, l'UIP nazionale si configura anche quale terminale unico per la ricezione di istanze formulate dalle autorità competenti, dalle UIP di altri Stati membri o da Europol, volte a ottenere i dati PNR o i risultati della loro elaborazione.

Si rammenta che i criteri direttivi recati dalla legge di delegazione europea n. 163 del 2017 prevedono che la UIP nazionale venga incardinata in seno al Dipartimento della pubblica sicurezza del Ministero dell'interno. In ossequio a tale criterio direttivo – che non autorizza l'istituzione di uffici dirigenziali generali *ad hoc* – il provvedimento prevede che l'organizzazione dell'Unità avvenga con gli strumenti tipici stabiliti dall'articolo 5, settimo comma, della legge n. 121 del 1981, ossia il decreto (organizzatorio) del Ministro dell'interno, di concerto con il Ministro dell'Economia e delle Finanze, con il quale vengono individuate competenze ed attribuzioni di uffici retti da Dirigenti Superiori o Primi Dirigenti della Polizia di Stato ed equiparati.

E' quindi rimessa, rispettivamente, ad un successivo decreto del Ministro dell'interno e ad un dPCM la definizione dei contingenti di personale, della Polizia di Stato e delle altre Forze di polizia, assegnato all'UIP. È, invece, affidato ad un 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 compito di provvedere all'organizzazione della struttura dell'UIP ed alla determinazione della relativa pianta organica.

L'**articolo 7** è dedicato al trattamento dei dati API, i quali, pur essendo parte dei dati PNR e venendo quindi trattati dall'UIP nazionale al pari degli altri dati contenuti

nel codice di prenotazione, devono essere altresì trattati, ai sensi della direttiva API, dagli Uffici incaricati di svolgere i controlli di polizia di frontiera per le finalità previste dalla stessa direttiva. Per rendere possibile tale operazione, il Sistema informativo è strutturato, da un punto di vista tecnico-operativo, in modo da consentire, una volta ricevuti i dati PNR, il trattamento dei dati PNR ad opera dell'UIP nazionale e il contestuale trattamento del sottoinsieme dei dati API da parte degli operatori di frontiera, nel rispetto delle condizioni e delle finalità previste dai rispettivi Atti comunitari.

L'**articolo 8** prevede un'analitica descrizione delle procedure di trattamento dei dati PNR, specificando le modalità operative tramite le quali l'UIP nazionale procede all'analisi delle informazioni. Tale analisi viene effettuata confrontando i dati PNR con le informazioni contenute nelle banche dati nazionali, europee e internazionali che possano fornire riscontri utili ai fini di prevenzione e repressione dei reati di terrorismo e dei reati gravi, ovvero trattando le informazioni sulla base di criteri predeterminati, individuati dalla stessa UIP nazionale e periodicamente aggiornati sentite le autorità competenti nazionali. Tanto nella fase più ampia dell'attività di analisi dei dati, quanto nella fase più specifica della determinazione dei criteri, viene dato ampio risalto alla necessità di rispettare il principio di non discriminazione.

La disposizione in esame definisce anche le condizioni per la successiva comunicazione di eventuali riscontri positivi alle autorità competenti nazionali, prevendendo un previo esame non automatizzato delle informazioni, condotto sul singolo caso e finalizzato a verificare la necessità dell'adozione di provvedimenti e misure da parte delle stesse autorità.

Si precisa, infine, che tali provvedimenti e misure non pregiudicano la possibilità di fare ingresso 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. Tale previsione è in linea con il principio generale, enunciato dalla direttiva PNR ("considerando" n. 34), per il quale rimangono impregiudicate le attuali norme unionali che regolano l'ingresso e l'uscita dal territorio comunitario e quelle che definiscono le modalità di effettuazione dei controlli alle frontiere.

L'**articolo 9** disciplina le modalità di trattamento dei dati API. Viene previsto che, immediatamente dopo la chiusura del volo, il Sistema informativo li rende consultabili da parte degli operatori di frontiera, per le finalità di prevenzione dell'immigrazione irregolare. I dati rilevanti per le citate finalità sono accessibili dagli Uffici di polizia di frontiera per un periodo di sei mesi dal loro trasferimento, mentre quelli irrilevanti sono resi non più visibili ai predetti Uffici entro ventiquattro ore dal momento della loro comunicazione, ovvero dopo l'ingresso dei passeggeri nel territorio dello Stato, in conformità alle disposizioni recate dalla direttiva API.

L'**articolo 10** è dedicato alla conservazione dei dati PNR e stabilisce, in sintesi, che tali dati, seppur conservati nel Sistema informativo per un periodo di cinque anni dal momento del loro trasferimento, siano trasformati in forma anonima allo scadere del sesto mese dal trasferimento stesso, mediante il mascheramento di specifici elementi idonei a identificare il soggetto cui si riferiscono.

Costituisce eccezione a tale regola generale l'ipotesi in cui le informazioni siano state trasferite a una delle Autorità competenti nazionali e rilevino nell'ambito di uno specifico caso di prevenzione e repressione di un reato di terrorismo o di un altro reato grave. In presenza di tali circostanze, il regime di conservazione delle informazioni segue le pertinenti disposizioni del codice di procedura penale, quelle vigenti in materia di trattamenti di dati personali per finalità di polizia, ovvero quelle riguardanti i trattamenti effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

La procedura di trasformazione in forma anonima determina riflessi sulla procedura di scambio informativo con le UIP di altri Stati membri e sul meccanismo di trasmissione dei dati o del risultato del loro trattamento alle autorità competenti (nazionali e straniere) e ad Europol. Infatti, se l'istanza volta a ottenere la trasmissione delle informazioni viene presentata decorsi i sei mesi, e quindi successivamente all'effettuazione dell'attività di mascheramento, l'UIP nazionale trasmette i dati solo in presenza di una richiesta debitamente motivata e previa autorizzazione dell'Autorità giudiziaria o del Vice Capo della polizia - Direttore centrale della polizia criminale, qualora si proceda nell'ambito di un procedimento penale o per l'applicazione di una delle misure di prevenzione disposte dall'Autorità giudiziaria ai sensi del Codice antimafia, ovvero per finalità di prevenzione.

L'**articolo 11**, coerentemente con la previsione di cui all'articolo 6 della direttiva API, disciplina l'obbligo dei vettori aerei di cancellare i dati API di cui dispongono entro ventiquattro ore dall'arrivo del volo.

Quest'ultima disposizione merita una riflessione ulteriore, con particolare riferimento all'assenza di un'omologa prescrizione in materia di dati PNR. Tale disallineamento trova fondamento, da un punto di vista formale, nell'assenza di una corrispondente previsione nella direttiva PNR e, da un punto di vista materiale, nella diversità di informazioni contenute nelle due tipologie di dati. I dati API comprendono sostanzialmente dati anagrafici e sono utilizzati per effettuare interrogazioni di banche dati al fine di individuare l'eventuale sussistenza di motivi ostativi all'ingresso dei passeggeri nel territorio dello Stato. Pertanto, una volta giunto il volo, non si ravvisano utilità per le quali i vettori aerei potrebbero continuare a conservare i dati API. I dati PNR, invece, comprendono una vasta gamma di informazioni, ben più ampie di quelle contenute nei dati API e, pertanto, potrebbero presentare profili di interesse per i vettori aerei nell'ambito di eventuali futuri riscontri o accertamenti necessari per affrontare contenziosi sorti nel corso dell'attività d'impresa.

Il **Capo III** prevede la regolamentazione del flusso informativo dei dati PNR e dei risultati del loro trattamento, in un'ottica di rafforzamento del meccanismo di condivisione delle informazioni e della cooperazione europea in materia di prevenzione e repressione dei fenomeni criminosi.

Più nel dettaglio, si disciplina, da un lato, la procedura di comunicazione delle informazioni a livello interno, ossia le modalità di cooperazione tra l'UIP nazionale e le autorità competenti nazionali (articolo 12) e, dall'altro, i meccanismi di comunicazione internazionale, ovverosia l'interscambio informativo tra l'UIP nazionale e le UIP o le Autorità competenti di altri Stati membri (articoli 13-17), oltreché il trasferimento dei dati a Europol (articolo 18) e ai Paesi terzi (articolo 19).

Gli **articoli 12 e 13** stabiliscono le modalità con le quali l'UIP nazionale trasmette i dati PNR o i risultati del loro trattamento, rispettivamente, alle autorità competenti nazionali e alle UIP di altri Stati membri, di propria iniziativa (in caso di riscontro positivo risultante dall'attività di analisi), ovvero come risposta ad una richiesta debitamente motivata dei predetti attori istituzionali, definendo le condizioni di ammissibilità della domanda.

Ai sensi dell'articolo 12, se l'UIP nazionale, all'esito del trattamento non automatizzato delle informazioni, rileva riscontri positivi, trasmette i dati PNR o il risultato del loro trattamento alle autorità competenti nazionali, consentendo a queste ultime di effettuare ulteriori verifiche e adottare le misure e i provvedimenti necessari a prevenire o reprimere reati di terrorismo o altri reati gravi. Tali provvedimenti, determinanti conseguenze giuridiche negative per l'interessato, non possono essere adottati esclusivamente sulla base del trattamento automatizzato dei dati PNR, né possono fondarsi su ragioni discriminatorie.

In alternativa al trasferimento delle informazioni d'iniziativa dell'UIP nazionale, si prevede la possibilità che, per le medesime finalità, le autorità competenti nazionali possano chiedere all'UIP nazionale la trasmissione dei dati PNR o dei risultati del loro trattamento.

Ai sensi dell'articolo 7, paragrafo 5, della direttiva PNR, l'ulteriore trattamento delle informazioni operato dalle autorità competenti "non pregiudica le competenze delle autorità di contrasto e giudiziarie nazionali qualora siano individuati altri reati o indizi di reato durante l'azione di contrasto determinata da tale trattamento".

L'attuazione di tale disposizione non sembra richiedere un'espressa norma di trasposizione nell'ordinamento interno, in virtù del generale principio del nostro sistema processuale per il quale, in assenza di espressi divieti, le informazioni possono essere utilizzate per le finalità, alle condizioni e con le modalità previste dalle pertinenti disposizioni in vigore.

Ai sensi dell'articolo 13, l'UIP nazionale, se rileva riscontri positivi, trasmette alle UIP di altri Stati membri le informazioni utili a prevenire o reprimere reati di terrorismo o altri reati gravi e, per le medesime finalità, è tenuta a trasmettere i dati

PNR o, se già effettuato, i risultati del trattamento, in caso di richiesta debitamente motivata proveniente dalle UIP estere.

Decorsi sei mesi dal trasferimento effettuato dai vettori aerei, e quindi una volta effettuata l'operazione di trasformazione dei dati PNR in forma anonima, l'UIP nazionale trasmette le informazioni alle condizioni previste dall'articolo 10, comma 3, ossia sulla base di una richiesta debitamente motivata e previa autorizzazione dell'Autorità giudiziaria o del Vice Capo della polizia - Direttore centrale della polizia criminale, qualora si proceda nell'ambito di un procedimento penale o per l'applicazione di una delle misure di prevenzione disposte dall'Autorità giudiziaria ai sensi del Codice antimafia, ovvero per finalità di prevenzione.

Nel caso di pericolo, imminente e concreto, che possa essere commesso un reato di terrorismo o un altro reato grave, per il quale si rende necessario ottenere i dati PNR di determinati voli prima delle tempistiche ordinarie, l'UIP estera può chiedere all'UIP nazionale di ottenere le informazioni in un momento antecedente al periodo compreso tra le ventiquattro e le quarantotto ore precedente l'orario previsto per la partenza del volo. In tal caso, l'UIP nazionale veicola l'istanza ai vettori aerei interessati, al fine di ottenere da questi ultimi le informazioni e diramarle alle UIP estere richiedenti.

L'**articolo 14** definisce i presupposti in presenza dei quali l'UIP nazionale è legittimata a trasmettere le informazioni direttamente alle autorità competenti di altri Stati membri, sancendo, implicitamente, il principio generale per il quale le autorità competenti di altri Stati membri, di regola, dialogano con l'UIP nazionale attraverso l'UIP del proprio Stato.

L'**articolo 15** disciplina le condizioni di procedibilità per la presentazione dell'istanza da parte dell'UIP nazionale volta ad ottenere la trasmissione dei dati PNR o del risultato del loro trattamento da parte dell'UIP di altro Stato membro, disponendo che la richiesta deve essere debitamente motivata in relazione a un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi.

Una volta ottenute le informazioni richieste, l'UIP nazionale effettua gli accertamenti di competenza e interessa, quando ne ricorrono le condizioni, le autorità competenti nazionali.

Si prevede, infine, la possibilità per l'UIP nazionale di ottenere le informazioni in anticipo rispetto al termine ordinario, parallelamente a quanto previsto per le UIP di altri Stati membri, applicando, a parti invertite, il medesimo meccanismo previsto dall'articolo 13.

L'**articolo 16** sancisce il principio generale secondo il quale le autorità competenti nazionali dialogano con l'UIP di altri Stati membri attraverso l'UIP nazionale e, a seguire, ne disciplina l'eccezione, prevedendo specifiche condizioni che legittimano le autorità competenti nazionali a rivolgersi direttamente all'UIP estera.

L'**articolo 17** si occupa delle modalità operative per lo scambio delle informazioni effettuato ai sensi degli articoli da 13 a 16, prescrivendo l'utilizzo di qualsiasi canale esistente di cooperazione internazionale di polizia.

Inoltre, il ruolo di punto di contatto italiano per la procedura d'emergenza viene attribuito all'UIP nazionale, essendo quest'ultima un'unità operante senza soluzione di continuità nell'arco delle ventiquattro ore.

L'articolo 18 stabilisce presupposti e modalità per la trasmissione dei dati PNR o dei risultati del loro trattamento a Europol. In particolare, quanto ai presupposti, l'UIP nazionale può trasferire le informazioni al citato organismo europeo in presenza di determinate condizioni e sulla base di una specifica istanza, veicolata tramite l'Unità Nazionale Europol e soggiacente a stringenti condizioni di ammissibilità. Quanto alle modalità, invece, la norma prevede che lo scambio delle informazioni tra l'UIP ed Europol avvenga attraverso l'applicazione SIENA (*Secure Information Exchange Network Application*), come richiesto dall'articolo 10, comma 4 della direttiva.

Tale articolo declina il "considerando" 24, secondo il quale la sicurezza dello scambio reciproco di informazioni relative ai dati PNR tra gli Stati membri dovrebbe essere garantita tramite uno dei canali di cooperazione esistenti tra le Autorità competenti degli Stati membri e, in particolare, con Europol tramite l'applicazione di rete per lo scambio di informazioni protetta, denominata SIENA. Tale rete è uno strumento ideato per consentire una comunicazione e uno scambio rapidi, sicuri e pratici di informazioni e di *intelligence* operative e strategiche riguardanti la criminalità fra Europol, gli Stati membri e i Paesi terzi con cui Europol ha concluso accordi di cooperazione.

L'**articolo 19** definisce i presupposti per la trasmissione dei dati PNR e dei risultati del loro trattamento ai Paesi terzi. A tal fine, viene riprodotta fedelmente la disciplina dettata dalla direttiva PNR, che viene, peraltro, arricchita di una necessaria precisazione: sono fatte salve le condizioni previste da eventuali accordi internazionali. Si specifica che il trasferimento dei dati PNR a Paesi terzi, in relazione a casi individuali, avviene in conformità alle previsioni, oltre che delle disposizioni del decreto, anche di quelle del Codice della *privacy*.

Il **Capo IV** reca disposizioni riguardanti la tutela dei dati personali oggetto dei trattamenti effettuati ai sensi del presente decreto.

I primi due articoli introducono e definiscono le due figure che rivestono un ruolo centrale sul piano della tutela del diritto di protezione dei dati personali di cui godono, ai sensi del Codice per la protezione dei dati personali, gli interessati e, nel caso di specie, i passeggeri le cui informazioni vengono trattate.

L'**articolo 20** stabilisce che l'autorità deputata a ricoprire il ruolo di Autorità nazionale di controllo, così come disciplinata dalla direttiva PNR, è il Garante per la protezione dei dati personali, il quale esercita l'attività di controllo sul trattamento dei

dati personali, ai sensi del quadro normativo vigente, e ha una funzione consultiva e di supporto nei confronti degli interessati relativamente all'esercizio dei loro diritti di protezione dei dati personali.

La disposizione richiama integralmente le disposizioni del Codice della *privacy* e quindi tutti i poteri di cui il Garante è titolare con riguardo ai trattamenti di dati per finalità di polizia o giudiziari. Peraltro, il rinvio operato è di natura "mobile" e consente di richiamare anche le previsioni che integreranno la disciplina di quel *corpus iuris* per effetto del recepimento della direttiva (UE) 2016/680. Si aggiunge che il provvedimento contiene ulteriori specificazioni dei poteri del Garante, per le quali si fa rinvio all'illustrazione dell'articolo 22.

L'**articolo 21** si occupa del responsabile della protezione dei dati, figura complementare a quella del Garante e parimenti essenziale nell'architettura complessiva del sistema di protezione dei dati, cui viene attribuito il fondamentale compito di vigilare sulla correttezza e sulla liceità del trattamento delle informazioni.

Il responsabile della protezione dei dati garantisce, inoltre, l'attuazione di tutte le misure tecniche e di sicurezza, nel rispetto di quanto disposto dal Codice per la protezione dei dati personali e funge da punto di contatto unico per gli interessati per tutte le questioni connesse al trattamento dei dati PNR che li riguardano.

La figura del responsabile della protezione dei dati è delineata in maniera differenziata rispetto a quelle del titolare e del responsabile del trattamento, di cui agli articoli 4, commi 1 e 2, e 21 del provvedimento. Tali differenti figure sono identificate in termini assolutamente *compliant* con le previsioni del Codice della *privacy*, che viene, infatti, richiamato. Il richiamo al Codice consente di escludere situazioni di confusione o sovrapponibilità con i compiti demandati al "responsabile della protezione dei dati" – figura assimilabile al *data protection officer* di cui al regolamento (UE) 2016/679 – ed all'UIP, i quali trovano il loro specifico "statuto" nelle previsioni della direttiva (UE) 2016/681.

Per quanto riguarda la sua posizione ordinamentale, se ne prevede la collocazione all'interno del Dipartimento di pubblica sicurezza, nell'ambito della Direzione centrale della polizia criminale, demandando la precipua individuazione a un successivo decreto del Capo della polizia – Direttore generale della pubblica sicurezza.

Tale scelta risponde a un'interpretazione sistematica e teleologicamente orientata delle pertinenti disposizioni della direttiva PNR, le quali postulano che il responsabile della protezione dei dati sia collocato in una posizione indipendente rispetto all'UIP nazionale. Ciò si evince, in particolare, dagli articoli 5, paragrafo 2, e 6, paragrafo 7, della direttiva, ai sensi dei quali il responsabile adempie alle proprie funzioni in modo efficace e indipendente e ha accesso a tutti i dati trattati dall'UIP. Tale soluzione evita che si verifichi una situazione di coincidenza dei compiti del "controllore" con quelli dell'organismo "controllato", garantendo, pertanto, che il responsabile operi nella prescritta posizione di indipendenza.

Detta strutturazione appare coerente rispetto a quella adottata da diversi altri Stati membri dell'Unione che, pur nelle differenze organizzative dovute alla diversa strutturazione del comparto sicurezza, hanno optato nelle loro scelte nel senso della valorizzazione delle caratteristiche di indipendenza del Responsabile per la protezione dei dati dalla struttura organizzativa dell'UIP, oggetto dell'attività di controllo da parte del Responsabile stesso. In particolare gli Stati nei quali l'implementazione della direttiva PNR risulta in fase più avanzata hanno inteso designare quale responsabile per la protezione dei dati figure al di fuori dell'UIP, al fine di meglio garantire l'indipendenza della funzione, istituendo unità organizzative (almeno) di pari livello gerarchico dell'UIP stessa.

Si prevede, infine, l'ovvia e auspicata attività di cooperazione e confronto tra le due figure cardine del sistema di protezione dei dati, attribuendo al responsabile la facoltà di rivolgersi al Garante nel caso dovesse rilevare ipotesi di trattamento illecito di dati.

L'**articolo 22** stabilisce che ai trattamenti dei dati personali effettuati in base al presente decreto si applicano le previsioni della Parte II, Titolo II, Capo I del Codice per la protezione dei dati personali, nonché del Titolo III, limitatamente ai trattamenti effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, e gli articoli da 33 a 36 del medesimo Codice al fine di assicurare l'attuazione delle misure di sicurezza necessarie a garantire la protezione dei dati.

Viene, poi, regolato l'obbligo per l'UIP di mettere a disposizione dell'*Authority* la documentazione afferente a sistemi e procedure di trattamento, nonché i registri delle attività compiute dall'UIP, come pure di comunicare al Garante i casi di *data breach*.

Si fa inoltre presente che le disposizioni del *Codice della privacy* si applicano tanto al trattamento dei dati effettuato dall'UIP nazionale, quanto al trattamento dei dati operato dai vettori aerei.

Questi ultimi, in particolare, devono adempiere all'obbligo di informativa previsto dall'articolo 13 del Codice e sono tenuti a adottare tutte le misure tecniche ed organizzative a tutela della sicurezza e della riservatezza dei dati.

L'UIP nazionale, godendo di un più ampio e incisivo potere di intervento sulle informazioni, è soggetta a oneri ulteriori rispetto all'adozione delle anzidette misure tecniche ed organizzative, individuabili, in sintesi, nell'obbligo di conservazione della documentazione relativa ai sistemi e alle procedure di trattamento e di appositi registri delle attività di raccolta, consultazione, comunicazione e cancellazione dei dati. La documentazione e i registri, a seguito di richiesta, devono essere messi a disposizione del Garante. Inoltre, l'UIP nazionale è tenuta a esercitare una funzione di "autocontrollo" in termini di correttezza del trattamento dei dati che effettua: se viene rilevata una violazione della disciplina in tema di protezione dei dati personali, l'Unità deve informarne, senza ritardo, l'interessato e il Garante.

Infine, a completamento del delineato sistema di protezione dei dati, si prevede il divieto per l'UIP nazionale di effettuare il trattamento con modalità tali da rivelare i dati sensibili dei passeggeri e, nell'ipotesi in cui tale situazione si dovesse di fatto

comunque verificare, si prescrive l'immediata cancellazione delle relative informazioni.

L'**articolo 23** chiude il Capo IV riconoscendo ai soggetti interessati dai trattamenti disciplinati dal presente decreto i diritti previsti dall'articolo 10, commi 3, 4 e 5 della legge n. 121 del 1981. Si prevede che i diritti siano esercitati previa presentazione di istanza alla Direzione centrale della polizia criminale, tramite la quale l'interessato può domandare che dell'esercizio di tali diritti venga data evidenza con l'apposizione di un'apposita indicazione (cd. "diritto di *flag*"). Tale indicazione può essere rimossa a richiesta dell'interessato o per effetto di un provvedimento adottato dal Garante ai sensi del Codice per la protezione dei dati personali.

Il **Capo V** reca la disciplina sanzionatoria e le disposizioni transitorie e finali.

In particolare, l'**articolo 24** prevede distinte ipotesi di violazione degli obblighi previsti dal presente decreto con conseguente individuazione delle autorità competenti a irrogare le rispettive sanzioni amministrative.

Nel caso di omesso, errato o incompleto trasferimento dei dati PNR da parte dei vettori aerei, la sanzione amministrativa è irrogata dall'ENAC nelle forme del procedimento previsto dalla legge 24 novembre 1981, n. 689, per ogni viaggio per il quale i dati dei passeggeri non sono stati comunicati o sono stati comunicati in modo errato o incompleto. Analoga sanzione è irrogata dall'ENAC in caso di mancato adempimento alle prescrizioni dettate dall'UIP nazionale per garantire la trasmissione dei dati PNR al Sistema Informativo.

Nel caso di omessa cancellazione dei dati API nel termine previsto dall'articolo 11, la sanzione amministrativa è irrogata dal Garante per la protezione dei dati personali, ai sensi dell'articolo 166 del relativo Codice.

È fatta salva, infine, 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.

L'**articolo 25** prevede l'onere di comunicare annualmente alla Commissione europea elaborazioni statistiche concernenti i dati PNR trasmessi all'UIP nazionale.

L'**articolo 26** detta la disciplina transitoria, vigente sino all'entrata in vigore dell'ultimo dei provvedimenti di attuazione chiamati a disciplinare, rispettivamente, il Sistema informativo, l'organizzazione della UIP nazionale e le modalità relative alla definitiva cancellazione dei dati PNR.

Inoltre, proprio in virtù dell'assorbimento della disciplina attuativa della direttiva API, e della conseguente previsione dell'unitaria trattazione dei dati PNR e dei dati API nella medesima piattaforma informatica, i riferimenti normativi al sistema informativo attualmente utilizzato per la gestione dei dati API (Sistema informativo frontaliero *Border Control System*) vengono sostituiti dai riferimenti al Sistema

Informativo di cui al presente decreto. Più in dettaglio, il Sistema informativo sostituirà materialmente il Sistema informativo frontaliero una volta entrato a completo regime, al fine di garantire l'imprescindibile continuità del servizio di analisi preventiva dei dati sui passeggeri, volta a prevenire il fenomeno dell'immigrazione irregolare.

Infine, l'**articolo 27** reca la clausola di neutralità finanziaria del provvedimento.

Relazione tecnica

La presente nota tecnica è volta a valutare gli effetti finanziari derivanti dal provvedimento indicato in epigrafe, al fine di verificare il rispetto della clausola di invarianza di spesa stabilita dall'articolo 12, comma 2, della Legge di delegazione europea 2016-2017 (Legge 25 ottobre 2017, n. 163).

Il provvedimento è emanato ai sensi del citato articolo 12, il quale delega il Governo a adottare un decreto legislativo per l'attuazione della Direttiva 27 aprile 2016, n. 2016/681/UE del Parlamento europeo e del Consiglio 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 (nel prosieguo, «Direttiva PNR»), il cui termine di recepimento scade il 25 maggio 2018.

Prima di entrare nel merito delle disposizioni recate dal decreto, occorre premettere che la Direttiva PNR si prefigge l'obiettivo di rafforzare il sistema di sicurezza europeo tramite mirati controlli sui flussi di passeggeri aerei all'interno e all'esterno dell'Unione Europea.

Tali controlli si sviluppano attraverso l'analisi di determinate informazioni, piuttosto ampie e elencate specificamente nell'allegato I della Direttiva (nel prosieguo, «dati PNR»), che ciascun passeggero fornisce ai vettori aerei in fase di prenotazione del volo. Si tratta di un insieme di dati che consente un'attività di analisi di assoluto rilievo, finalizzata all'individuazione di passeggeri sospettati di essere implicati in reati di terrorismo o in altri reati gravi.

Il trattamento delle informazioni e le connesse attività saranno svolti dall'Unità d'informazione sui passeggeri (UIP) nazionale, ossia dall'unità appositamente istituita presso la Direzione Centrale della Polizia Criminale del Dipartimento della pubblica sicurezza del Ministero dell'Interno, ai fini dell'analisi dei dati PNR, per la quale si rinvia al prosieguo della trattazione (articolo 6).

Per l'effettuazione di tale attività di analisi è stato istituito apposito Sistema Informativo presso il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno, attraverso il quale i dati PNR vengono raccolti e trattati, ai sensi dell'**articolo 4** del presente decreto.

Il Sistema Informativo consente la contestuale gestione delle informazioni sui passeggeri acquisite ai sensi della Direttiva 29 aprile 2004, n. 2004/82/CE (nel prosieguo «dati API») ed è destinato quindi a sostituire, a completo regime, il Sistema informativo frontaliero *Border Control System* (BCS), attualmente utilizzato dagli Uffici incaricati dei controlli di polizia di frontiera per le finalità e alle condizioni previste dalla citata Direttiva (nel prosieguo, «Direttiva API»).

In particolare, la soluzione tecnica da realizzare si concretizza in una piattaforma informatica unitaria per garantire un'efficace, efficiente ed economica gestione dei dati PNR e dei dati API, da realizzare presso il Centro Elettronico Nazionale della Polizia di Stato di Napoli, con connessione al sito di *Disaster Recovery* presso il Centro Polifunzionale di Bari.

Ai fini dell'attuazione della Direttiva PNR, la Legge 11 dicembre 2016, n. 232, "Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019", all'articolo 1, comma 608, ha stanziato 5,5 milioni di euro per l'anno 2017, 16

milioni di euro per l'anno 2018 per la realizzazione della piattaforma informatica e 4,5 milioni di euro a decorrere dall'anno 2019 per la gestione e la manutenzione della stessa.

Le risorse previste dal predetto articolo 1, comma 608, sono state allocate sui seguenti capitoli di spesa:

- Cap. 7505 "Spese per la realizzazione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)" – parte capitale.
  Anno 2017 – euro 5.500.000
  Anno 2018 – euro 16.000.000
  Anno 2019 - 0
- Cap. 2563 "Spese per la gestione e la manutenzione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)" – parte corrente.
  Anno 2017 – 0
  Anno 2018 – 0
  Anno 2019 – euro 4.500.000.

La Legge 27 dicembre 2017, n. 205, "Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020" ha quindi disposto i seguenti stanziamenti:

- Cap. 7505 "Spese per la realizzazione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)"
  Anno 2018 – euro 16.000.000
  Anno 2019 – 0
  Anno 2020 - 0
- Cap. 2563 "Spese per la gestione e la manutenzione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)"
  Anno 2018 – 0
  Anno 2019 – euro 4.500.000
  Anno 2020 – euro 4.500.000.

Si soggiunge che, con la decisione di esecuzione del 18 settembre 2017, la Commissione europea ha reso disponibili ulteriori risorse sul Fondo Sicurezza Interno – Programma Nazionale dell'Italia (ISF) pari a euro 5.988.253, per il 50% di quota europea, ai fini della specifica attuazione della Direttiva (UE) 681/2016. Conseguentemente, tali risorse, unitamente a quelle di pari entità cofinanziate dall'Italia, hanno consentito di progettare la realizzazione di ulteriori funzioni necessarie ad elevare l'efficienza dell'infrastruttura tecnologica destinata al trattamento dei dati PNR e alle connesse attività dell'UIP nazionale.

Le accresciute disponibilità e una più puntuale definizione del quadro esigenziale emerso nel corso delle attività di programmazione e realizzazione del sistema hanno determinato una rimodulazione del progetto inizialmente delineato da questa Amministrazione.

In questo senso, è stato possibile accuratizzare il progetto, prevedendo la possibilità di:

- disporre di dati omogenei certificati relativi alla totalità dei voli intra-UE e extra-UE, in ingresso e in uscita dal territorio nazionale;
- acquisire un sofisticato software *ad hoc* dotato di numerose funzioni in grado di supportare in modo più efficace l'attività di analisi di dati PNR in relazione alla tipologia di reati che la Direttiva PNR mira a prevenire e contrastare.

In tale contesto, si evidenzia che nelle ipotesi iniziali era stato previsto di destinare una quota pari a euro 7.500.000 a gravare sui fondi stanziati dall'articolo 1, comma 608, della Legge 11 dicembre 2016, n. 232, per la realizzazione dei collegamenti tra il CEN di Napoli e il CED interforze – al fine di garantire l'ampliamento della connettività nonché la sicurezza del trasporto delle informazioni - necessari al più efficace funzionamento della piattaforma PNR. Considerato, tuttavia, che tali interventi costituiscono una realizzazione "a fattor comune" anche per altre funzionalità dell'Amministrazione della pubblica sicurezza, è emersa la necessità di ricorrere, indipendentemente dal progetto PNR, alle risorse previste dall'articolo 1, comma 140, della Legge 232/2016, a seguito di ripartizione dell'apposito fondo, avvenuta alla fine dell'anno 2017.

Conseguentemente, ciò ha "liberato" euro 7.500.000 previsti dall'articolo 1, comma 608, della Legge di bilancio 2016, che si programma di impiegare sempre per il progetto PNR, accrescendone le funzionalità e le potenzialità operative.

Ciò premesso, si riportano gli elementi che hanno portato alla quantificazione dei fabbisogni.

Per quanto riguarda i fondi ordinari di conto capitale stanziati dalla citata Legge n. 232 del 2016, pari a euro 21.500.000, in relazione alle annualità 2017 e 2018, sono stati attualmente impegnati circa euro 20.850.000 (comprensivi di IVA), secondo il seguente dettaglio:

- acquisto del servizio di ricezione di dati PNR e API qualificati e omogenei per un totale di euro 6.908.000;
- realizzazione del software per la gestione dei dati API: euro 9.600.000 per il software centralizzato, più euro 1.740.000 per il software degli Uffici di frontiera;
- acquisto del servizio di conduzione del sistema API/PNR per un totale di euro 2.600.000;

Per quanto concerne i fondi ISF, le somme saranno così ripartite:

- realizzazione software per la gestione dei dati PNR: euro 5.500.000;
- fornitura hardware e software a licenza per una spesa pari a euro 5.300.000, di cui:
  - realizzazione infrastruttura presso C.E.N. di Napoli ove sarà attestata la struttura centrale: euro 4.800.000;
  - esigenza di adeguamento dell'hardware per la sala server della Direzione Centrale della Polizia Criminale, presso la quale si attesterà l'UIP: euro 500.000;
- potenziamento dell'infrastruttura tecnologica necessario per garantire l'operatività dell'UIP nazionale (fornitura di hardware e software di base): euro 220.000.

Il quadro complessivo delle risorse, come sopra delineato, garantisce quindi che il recepimento della Direttiva PNR non richiede ulteriori interventi capaci di generare effetti di spesa: l'adeguamento dell'ordinamento interno sarà attuato con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Infatti, ad eccezione dei costi derivanti dalla realizzazione del Sistema Informativo, il decreto introduce norme di carattere procedurale e di natura ordinamentale o, comunque, norme la cui attuazione non richiede interventi tali da comportare nuovi o ulteriori dispendi di risorse pubbliche, come qui di seguito illustrato segnatamente per ogni disposizione.

Articoli 1, 2 e 3 (obiettivo, ambito di applicazione, definizioni e finalità dei trattamenti)

L'articolo 1 enuncia l'obiettivo dell'intervento normativo (attuazione della Direttiva PNR e assorbimento della normativa di attuazione della Direttiva API) e ne definisce l'ambito di applicazione.

L'articolo 2 detta norme di carattere definitorio, mentre l'articolo 3 enuncia le specifiche finalità per le quali deve essere effettuato il trattamento dei dati PNR e dei dati API.

Si tratta, quindi, di previsioni puramente ordinamentali, insuscettibili di determinare nuovi o ulteriori oneri a carico della finanza pubblica.

Articolo 4 (Sistema Informativo)

L'articolo 4 disciplina la realizzazione del Sistema Informativo dedicato alla trattazione dei dati PNR e dei dati API (comma 1). Per i profili di spesa riguardanti la creazione di tale *repository*, oltre a quanto già esplicitato in premessa, si specifica che tale attività prevede l'acquisto di un servizio per la realizzazione di un software *ad hoc* per la gestione dei dati API e PNR, nonché per la fornitura dell'hardware e del software a licenza.

Gli oneri per l'acquisto, pari a euro 9.600.000, sono imputati sul capitolo di bilancio 7505 di parte capitale, con riferimento al trattamento centralizzato dei dati API, e pari a euro 5.500.000, a valere sui fondi ISF, con riferimento al trattamento dei dati PNR.

Ulteriori oneri, pari a euro 2.600.000 a valere sul capitolo 7505, sono previsti per il servizio di conduzione operativa del Sistema informativo.

L'attuazione della disposizione comporta, infine, una spesa pari a euro 1.700.000 per l'acquisto dell'hardware, e una spesa pari a euro 3.820.000 per l'acquisto dei software a licenza, a valere sui fondi ISF.

Le disposizioni di cui ai commi 2, 3 e 4 regolano le condizioni di utilizzo del sistema e l'individuazione del titolare e dei responsabili del trattamento dei dati PNR e dei dati API. Si tratta di norme ordinamentali la cui attuazione non comporta nuovi o ulteriori oneri a carico del bilancio dello Stato.

Articolo 5 (implementazione del Sistema Informativo)

L'articolo 5 sancisce l'obbligo per i vettori aerei di trasferire i dati PNR al Sistema Informativo e ne prevede le specifiche modalità di adempimento.

La norme disciplina dunque oneri ad esclusivo carico dei predetti operatori economici ed è quindi insuscettibile di determinare conseguenze negative per la finanza pubblica.

Articolo 6 (Unità d'informazione sui passeggeri nazionale)

L'articolo 6 prevede che l'organizzazione dell'UIP nazionale sia definita con l'ordinario strumento del decreto del Ministro dell'Interno, adottato di concerto con il Ministro dell'Economia e della Finanze ai sensi dell'articolo 5, settimo comma, della Legge n. 121/1981 e la dotazione organica, anche della componente interforze, sia stabilita con il decreto del Presidente del Consiglio dei Ministri di cui all'articolo 6, secondo comma, della stessa Legge n. 121/1981. A riguardo si precisa che l'adozione di tali provvedimenti non implicherà nuovi o ulteriori aggravi a carico della finanza pubblica, in quanto ai nuovi fabbisogni di personale si provvederà con le risorse disponibili a legislazione vigente.

Sul punto, si precisa che la Direzione Centrale della Polizia Criminale dispone di una dotazione effettiva pari complessivamente a 1.052 unità (dato aggiornato al 16 novembre scorso), delle varie qualifiche e ruoli delle quattro Forze di polizia, oltreché dell'Amministrazione civile dell'Interno. Tale dotazione appare adeguata alle esigenze, alla luce del fatto che eventuali moderati bisogni di incremento del numero di personale possono essere soddisfatti attingendo ad altre articolazioni del Dipartimento della pubblica sicurezza, che conta oggi su un organico effettivo pari a circa 7.500 unità.

Il comma due reca norme di natura procedurale e come tali insuscettibili di determinare ulteriori oneri.

Articolo 7 (Uffici incaricati dei controlli di polizia di frontiera)

L'articolo 7 disciplina il trattamento dei dati API ad opera degli Uffici incaricati dei controlli di polizia di frontiera, configurando una delle tappe del processo di assorbimento, realizzato dal presente decreto, della normativa di attuazione della Direttiva API.

I dati API vengono attualmente trattati attraverso il Sistema informativo frontaliero *Border Control System* che, come anticipato in premessa, verrà sostituito dal Sistema Informativo di cui al presente decreto una volta entrato in funzione a pieno regime. Pertanto, i costi connessi alla messa a punto degli strumenti tecnici per il trattamento dei dati API effettuato dagli operatori di frontiera ammontano a euro 1.740.000, a valere sul capitolo 7505.

Il personale che effettuerà il trattamento dei dati API ai sensi del presente decreto è lo stesso che opera attualmente e, di conseguenza, l'attuazione di tale disposizione sarà assicurata con le risorse umane disponibili a legislazione vigente.

Articolo 8 e 9 (trattamento dei dati PNR e dei dati API)

Gli articoli 8 e 9 definiscono le modalità operative del trattamento dei dati PNR e dei dati API. Nell'ambito dei costi derivanti dalla realizzazione del Sistema Informativo utilizzato per la raccolta e il trattamento di entrambe le tipologie di dati, di cui si è parlato dettagliatamente in premessa e *sub* articolo 4, l'attività di trattamento dei dati PNR e API comporta l'acquisizione di un servizio che consenta di ricevere dati PNR e API qualificati e omogenei. Gli oneri per l'acquisto, pari a euro 6.908.000, sono imputati sul già citato capitolo di bilancio 7505 di parte capitale.

Gli articoli in esame, inoltre, dettano norme di carattere procedurale, dalla cui attuazione non derivano nuovi o ulteriori profili di spesa.

Articolo 10 (periodo di conservazione dei dati PNR e trasformazione in forma anonima)

L'articolo 10 regola le modalità di conservazione, di trasformazione in forma anonima e di cancellazione dei dati PNR e dei risultati del loro trattamento. Tali attività saranno garantite mediante il software *ad hoc* citato *sub* articolo 4, la cui copertura finanziaria sarà garantita mediante il ricorso ai fondi ISF.

Si disciplinano altresì le condizioni per il trasferimento delle informazioni alle autorità competenti e a Europol decorsi i sei mesi dalla trasmissione delle informazioni da parte dei vettori aerei, ossia una volta che è stata effettuata la procedura di mascheramento dei dati. Si

prevedono passaggi procedurali che costituiscono adempimenti di ridotta complessità e che pertanto non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Articolo 11 (conservazione dei dati API)

L'articolo 11, conformemente all'articolo 6 della Direttiva API, dispone l'obbligo per i vettori aerei di cancellare, entro ventiquattro ore dall'arrivo del volo, i dati API trasmessi. Si tratta dell'attribuzione di un onere, peraltro già vigente, a carico dei vettori aerei, insuscettibile di determinare aggravi per il bilancio dello Stato.

Articolo 12 (trasferimento dei dati PNR alle autorità competenti nazionali)

L'articolo 12 definisce le modalità con le quali l'UIP nazionale trasmette, d'iniziativa ovvero sulla base di una richiesta debitamente motivata, i dati PNR e i risultati del loro trattamento alle autorità competenti nazionali, prescrivendo l'utilizzo di strumenti informatici, secondo quanto previsto con i decreti di natura non regolamentare di cui all'articolo 4, comma 5, inerenti al funzionamento tecnico del Sistema Informativo e quindi dotati della copertura finanziaria indicata per l'articolo 4.

Per le trasmissioni dei dati in parola, così come per le trasmissioni previste dagli articoli da 13 a 18, sarà utilizzato il sistema SIENA, ovvero i consueti canali sicuri e protetti (PEC, MIC), nonché ogni altro canale di cooperazione internazionale di polizia, attraverso i quali già oggi si sviluppano le comunicazioni tra la Direzione Centrale della Polizia Criminale, presso la quale sarà istituita l'UIP nazionale, e le autorità. Atteso che i suddetti canali sostengono, ad oggi, un traffico in entrata e in uscita pari a circa 600.000 messaggi all'anno e che tali applicazioni sono in grado di supportare, senza inconvenienti, un incremento stimato del 15% nel triennio, si ritiene che tali strutture siano in grado di far fronte al flusso derivante dal trattamento dei dati PNR.

Le restanti previsioni della disposizione rivestono carattere eminentemente ordinamentale e procedurale e non comportano l'insorgenza di nuovi o ulteriori oneri per la finanza pubblica.

Articoli da 13 a 17 (scambio di dati PNR con le autorità competenti e con le UIP di altri Stati membri)

Gli articoli da 13 a 16 disciplinano le procedure e le condizioni in presenza delle quali l'UIP nazionale trasferisce o scambia i dati PNR e i risultati del loro trattamento con le autorità competenti e con le UIP di altri Stati membri. Si tratta di disposizioni aventi tenore procedurale, che presenterebbero profili di spesa solo nell'eventualità in cui si dovessero creare *ex novo* canali di comunicazione specificamente dedicati alla trasmissione reciproca dei dati PNR tra i citati attori istituzionali.

Tale eventualità è esclusa dalla previsione di cui all'articolo 17, che prescrive l'utilizzo dei canali di cooperazione internazionale di polizia già esistenti. Pertanto, la disposizione non comporta nuovi o maggiori oneri a carico della finanza pubblica.

Articolo 18 (trasferimento dei dati PNR a Europol)

L'articolo 18 detta le condizioni per il trasferimento dei dati PNR o dei risultati del loro trattamento a Europol.

Al verificarsi dei presupposti prescritti, l'UIP nazionale trasmette le informazioni a Europol utilizzando l'applicazione SIENA secondo le disposizioni di cui al regolamento (CE) 11 maggio 2016, n. 2016/794.

Anche in questo caso si prescrive l'utilizzo di un meccanismo di comunicazione già esistente e pertanto, in relazione ai profili di carattere finanziario, si richiamano le osservazioni formulate poco sopra per gli articoli dedicati al trasferimento e allo scambio delle informazioni con gli Stati membri e si escludono nuovi aggravi per il bilancio dello Stato.

Articolo 19 (trasferimento dei dati PNR ai Paesi terzi)

L'articolo 19 si occupa del trasferimento dei dati PNR e dei risultati del loro trattamento ai Paesi terzi, subordinandolo al verificarsi di stringenti presupposti e facendo salve le condizioni previste da eventuali accordi internazionali.

La norma contiene disposizioni di natura ordinamentale e non determina ricadute sui livelli della spesa pubblica, atteso che la trasmissione dei dati rientra nell'ordinaria attività di cooperazione giudiziaria e di polizia.

Articolo 20 (autorità nazionale di controllo)

L'articolo 20 individua l'"Autorità nazionale di controllo" (così come delineata dalla Direttiva PNR) nel Garante per la protezione dei dati personali e attribuisce espressamente allo stesso l'esercizio della funzione di controllo con le modalità previste dal Codice in materia di protezione dei dati personali.

Si tratta di una disposizione di carattere ordinamentale, che non attribuisce al Garante compiti ulteriori rispetto a quelli espletati nell'ambito delle ordinarie attività istituzionali e non comporta quindi nuovi o ulteriori oneri per la finanza pubblica.

Articolo 21 (responsabile per la protezione dei dati)

L'articolo 21 introduce la figura del responsabile della protezione dei dati e ne disciplina le attribuzioni e la posizione ordinamentale, collocandolo nell'ambito della Direzione Centrale della Polizia Criminale del Dipartimento della pubblica sicurezza del Ministero dell'Interno. La designazione dello specifico ufficio competente a svolgere le funzioni di responsabile della protezione dei dati si perfezionerà con un successivo decreto del Capo della Polizia – Direttore Generale della Pubblica Sicurezza, la cui attuazione sarà assicurata con le risorse umane e strumentali disponibili a legislazione vigente e, pertanto, a invarianza di spesa pubblica (si fa rinvio a quanto già illustrato relativamente all'articolo 6).

Articolo 22 (protezione dei dati personali)

L'articolo 22 stabilisce che in relazione ai trattamenti dei dati personali effettuati ai sensi del presente decreto trovano applicazione le misure già oggi contemplate dalle disposizioni del Codice per la protezione dei dati personali.

Si prescrivono anche specifici oneri per l'UIP nazionale volti a garantire la correttezza del trattamento dei dati e il rispetto delle norme previste in materia di protezione dei dati personali.

Si tratta di previsioni di carattere procedurale che non richiedono interventi tali da determinare ulteriori costi a carico del bilancio dello Stato, alla luce di quanto già riferito relativamente all'articolo 6.

Articolo 23 (diritti degli interessati)

L'articolo 23 riconosce ai soggetti interessati dai trattamenti di dati personali, effettuati nel contesto regolato dal presente decreto, i diritti che già oggi prevede l'articolo 10, commi 3, 4 e 5, della Legge 1 aprile 1981, n. 121, in relazione alle informazioni conservate nel Centro elaborazione dati. Sul punto, si precisa che le istanze presentate ai sensi del citato articolo 10, in relazione ai dati PNR, saranno trattate dal competente ufficio della Direzione Centrale della Polizia Criminale, il cui carico di lavoro ammonta attualmente a circa 6.100 istanze all'anno. Tale carico di lavoro è riferito a una mole di trattamenti effettuati dalle Forze di polizia significativamente cospicua. Rispetto a tale volume, l'incremento del numero di istanze, sebbene non quantificabile in termini esatti a priori, può considerarsi contenuto, sia in termini numerici, sia in termini di impegno richiesto. Ciò in quanto le questioni che potranno essere dibattute saranno riferite ad un numero naturalmente esiguo di soggetti "a rischio", e comunque richiederanno come verifica negli archivi di polizia dell'esistenza o meno di iscrizioni pregiudizievoli, ovvero di altre ricorrenze particolarmente significative.

Alla luce di ciò, l'incremento di attività amministrative derivante, su questo versante, dal provvedimento all'esame non determina nuovi o maggiori oneri a carico della finanza pubblica. Ciò anche alla luce di volumi organici della Direzione Centrale della Polizia Criminale e dell'intero Dipartimento della Pubblica Sicurezza descritti *sub* articolo 6.

Inoltre, viene riconosciuto all'interessato il diritto che sia data evidenza nel Sistema Informativo dell'esercizio dei propri diritti. Si tratta di una misura la cui implementazione non richiede interventi tali da determinare nuovi dispendi di risorse pubbliche.

Analoghe considerazioni valgono per le disposizioni ai sensi delle quali all'interessato devono essere comunicati i provvedimenti adottati a seguito dell'esercizio dei propri diritti e per le quali il Garante può disporre la rimozione dell'indicazione della citata evidenza nel Sistema Informativo.

Articolo 24 (sanzioni)

L'articolo 24 definisce le violazioni al presente decreto che rilevano ai fini sanzionatori, individuando le specifiche sanzioni amministrative e le autorità competenti a irrogarle.

Più in dettaglio, seppur con un aggravio nel trattamento sanzionatorio, viene sostanzialmente mutuato il meccanismo introdotto dalla normativa di attuazione della Direttiva API, già operante e, pertanto, insuscettibile di determinare l'insorgenza di nuovi o ulteriori aggravi per il bilancio dello Stato.

Articolo 25 (statistiche)

L'articolo 25 prevede l'onere per il Ministero dell'Interno di comunicare, annualmente, alla Commissione europea determinati dati statistici concernenti i dati PNR trasmessi all'UIP nazionale, senza determinare, in fase attuativa, nuovi dispendi di risorse pubbliche.

Articolo 26 (disposizioni transitorie e finali)

L'articolare 26 norma l'entrata in vigore del presente decreto e detta norme transitorie per il periodo necessario all'adozione dei provvedimenti attuativi.

La disposizione introduce altresì norme di coordinamento con la disciplina di attuazione della Direttiva API, resesi necessarie in considerazione dell'assorbimento della disciplina stessa disposto dall'articolo 1.

Articolo 27 (clausola di neutralità finanziaria)

Reca la clausola di neutralità finanziaria in coerenza con quanto stabilito dall'articolo 12, comma 2, della Legge di delegazione europea 2016-2017.

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196, ha avuto esito

[X] POSITIVO [ ] NEGATIVO

Il Ragioniere Generale dello Stato

21 FEB. 2018

DIRETTIVA	LEGISLAZIONE NAZIONALE	COMMENTO
Articolo 1 Oggetto e ambito di applicazione 1. La presente direttiva prevede: a) il trasferimento a cura dei vettori aerei dei dati del codice di prenotazione dei passeggeri (PNR) dei voli extra-UE; b) il trattamento dei dati di cui alla lettera a), comprese le operazioni di raccolta, uso e conservazione a cura degli Stati membri e il loro scambio tra gli Stati membri. 2. I dati PNR raccolti a norma della presente direttiva possono essere trattati unicamente a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, secondo quanto previsto all'articolo 6, paragrafo 2, lettere a), b) e c).	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 (art. 12) Decreto legislativo 2 agosto 2007, n. 144, recante l'attuazione della Direttiva 2004/82/CE, concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate (artt. 3 e 4); Decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, e successive modificazioni (artt. 3, 53, 57).	L'art. 1, paragrafo 1, della direttiva definisce l'ambito d'applicazione dell'atto comunitario, e cioè l'obbligo per i vettori aerei di trasmettere i dati del codice di prenotazione dei passeggeri (PNR) dei voli extra-UE e del relativo trattamento dei dati. Il paragrafo 2 della direttiva stabilisce il limite delle finalità stabilendo che i dati PNR possono essere trattati, rispettivamente, al fine di prevenire e reprimere reati di terrorismo o altri reati gravi Gli obiettivi perseguiti dalla direttiva sono richiamati dall'art. 1, comma 1, e dall'art. 3, comma 1 dello schema di decreto.
Articolo 2 Applicazione della presente direttiva ai voli intra-UE 1. Se uno Stato membro decide di applicare la presente direttiva ai voli intra-UE, lo notifica per iscritto alla Commissione. Uno Stato membro può effettuare o revocare tale notifica in qualsiasi momento. La Commissione pubblica tale notifica e ogni sua eventuale revoca nella Gazzetta ufficiale dell'Unione europea.	Decreto legislativo 2 agosto 2007, n. 144, recante l'attuazione della Direttiva 2004/82/CE, concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate (art. 3).	L'art. 2, paragrafo 1, della direttiva prevede che gli Stati membri dell'UE che ne facciano richiesta possano applicare la citata direttiva anche per i voli intra-UE. Con la presente disposizione si intendono completare gli obiettivi di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Gli obiettivi perseguiti dalla direttiva sono richiamati dall'art. 1, comma 1, dello

2. Qualora sia effettuata una notifica di cui al paragrafo 1, tutte le disposizioni della presente direttiva si applicano ai voli intra-UE come se fossero voli extra-UE e ai dati PNR riguardanti voli intra-UE come se fossero dati PNR riguardanti voli extra-UE. 3. Uno Stato membro può decidere di applicare la presente direttiva solo a voli intra-UE selezionati. Nell'adottare tale decisione, lo Stato membro seleziona i voli che ritiene necessari per perseguire gli obiettivi della presente direttiva. Lo Stato membro può decidere di modificare la selezione dei voli intra-UE in qualsiasi momento		schema di decreto.
Articolo 3 Definizioni Ai fini della presente direttiva si intende per: 1) «vettore aereo», un'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; 2) «volo extra-UE», un volo di linea o non di linea effettuato da un vettore aereo in provenienza da un paese terzo e che deve atterrare nel territorio di uno Stato membro oppure in partenza dal territorio di uno Stato membro e che deve atterrare in un paese terzo, compresi, in entrambi i casi, i voli con scali nel territorio di Stati membri o di paesi terzi;	Decreto legislativo 2 agosto 2007, n. 144, recante l'attuazione della Direttiva 2004/82/CE, concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate (art. 2).	Le norme definitorie di cui all'articolo 3 della direttiva sono recepite dall'art. 2 dello schema di decreto, che ne contiene di ulteriori.

3) «volo intra-UE», un volo di linea o non di linea effettuato da un vettore aereo in provenienza dal territorio di uno Stato membro e che deve atterrare nel territorio di uno o più altri Stati membri, senza alcuno scalo nel territorio di un paese terzo; 4) «passeggero», chiunque, compresi i passeggeri in trasferimento o in transito ed esclusi i membri dell'equipaggio, sia trasportato o da trasportare in un aeromobile con il consenso del vettore aereo, risultante dalla registrazione di tali passeggeri nell'elenco dei passeggeri; 5) «codice di prenotazione» o «PNR», le informazioni relative al viaggio di ciascun passeggero comprendenti i dati necessari per il trattamento e il controllo delle prenotazioni a cura dei vettori aerei e di prenotazione interessati per ogni volo prenotato da qualunque persona o per suo conto, siano esse registrate in sistemi di prenotazione, in sistemi di controllo delle partenze utilizzato per la registrazione dei passeggeri sui voli, o in altri sistemi equivalenti con le stesse funzionalità; 6) «sistema di prenotazione», il sistema interno del vettore aereo in cui sono raccolti i dati PNR ai fini della gestione delle prenotazioni;		

7) «metodo push», il metodo in base al quale i vettori aerei trasferiscono i dati PNR elencati nell'allegato I alla banca dati dell'autorità richiedente; 8) «reati di terrorismo», i reati ai sensi del diritto nazionale di cui agli articoli da 1 a 4 della decisione quadro 2002/475/GAI; 9) «reati gravi», i reati elencati nell'allegato II, che siano punibili con una pena detentiva o una misura di sicurezza privativa della libertà personale non inferiore a tre anni conformemente al diritto nazionale di uno Stato membro; 10) «rendere anonimo mediante mascheratura degli elementi dei dati», rendere invisibili per un utente quegli elementi dei dati che potrebbero servire a identificare direttamente l'interessato.		
Articolo 4 Unità d'informazione sui passeggeri 1. Ciascuno Stato membro stabilisce o designa un'autorità competente in materia di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, o una sua sezione, che agisca in qualità di «unità	Legge 1 aprile 1981, n. 121 Nuovo ordinamento dell'Amministrazione della pubblica sicurezza (artt. 5, 6, 16).	L'articolo 4 della direttiva stabilisce che ogni Stato membro designi l'autorità competente (UIP) in materia di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, cui è affidato l'incarico di raccogliere, conservare, trattare e trasferire i dati PNR. L'art. 4, comma 2, dello schema di decreto affida, così come stabilito dal Codice della

d'informazione sui passeggeri» (UIP). 2. La UIP è incaricata di: a) raccogliere i dati PNR presso i vettori aerei, conservare, trattare e trasferire tali dati o i risultati del loro trattamento alle autorità competenti di cui all'articolo 7; b) scambiare sia i dati PNR che i risultati del trattamento di tali dati con le UIP degli altri Stati membri e con Europol conformemente agli articoli 9 e 10. 3. I membri del personale delle UIP possono essere funzionari distaccati delle autorità competenti. Gli Stati membri dotano le UIP delle risorse adeguate per svolgere i loro compiti. 4. Due o più Stati membri (Stati membri partecipanti) possono istituire o designare una stessa autorità che agisca in qualità di UIP. Tale UIP è stabilita in uno degli Stati membri partecipanti ed è considerata la UIP di tutti gli Stati membri partecipanti. Gli Stati membri partecipanti ne concordano congiuntamente le modalità di funzionamento e rispettano le prescrizioni di cui alla presente direttiva. 5. Entro un mese dall'istituzione del suo UIP ciascuno Stato membro ne dà notifica alla Commissione e può modificare la sua notifica		privacy, le funzioni di responsabile del trattamento a due diverse articolazioni del Dipartimento della Pubblica Sicurezza: Polizia Criminale (con riferimento ai dati PNR) e Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere (per quanto riguarda i dati API). L'art. 4, paragrafo 2, della direttiva è disciplinata dall'art. 6 dello schema di decreto.

in qualsiasi momento. La Commissione pubblica la notifica e le eventuali modifiche della stessa nella Gazzetta ufficiale dell'Unione europea.		
Articolo 5 Responsabile della protezione dei dati all'interno dell'UIP 1. L'UIP nomina un responsabile della protezione dei dati incaricato di sorvegliare il trattamento dei dati PNR e di attuare le pertinenti garanzie. 2. Gli Stati membri forniscono al responsabile della protezione dei dati i mezzi per adempiere alle funzioni e ai compiti che gli incombono a norma del presente articolo in modo efficace e indipendente. 3. Gli Stati membri assicurano che gli interessati abbiano il diritto di contattare il responsabile della protezione dei dati, che funge da punto di contatto unico, in merito a tutte le questioni connesse al trattamento dei dati PNR che li riguardano.		L'articolo 5, paragrafo 1, della direttiva, attribuisce all'UIP il compito di nominare il responsabile della protezione dei dati incaricato di sorvegliare il trattamento dei dati PNR e di attuare le pertinenti garanzie.
Articolo 6 Trattamento dei dati PNR 1. I dati PNR trasferiti dai vettori aerei sono raccolti dall'UIP dello Stato membro interessato secondo quanto previsto all'articolo 8. Qualora nei dati PNR trasferiti dai vettori aerei siano compresi dati diversi da quelli elencati nell'allegato I, l'UIP li cancella in via definitiva non appena li riceve.	Decreto legislativo 2 agosto 2007, n. 144, recante l'attuazione della Direttiva 2004/82/CE, concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate (artt. 3 e 4).	L'articolo 6 della direttiva disciplina dettagliatamente come deve avvenire il trattamento dei dati PNR, affidato all'UIP. L'articolo della direttiva è ripreso dagli articoli 6, comma 2, 8, 12, comma 1 dello schema di decreto.

2. L'UIP provvede al trattamento dei dati PNR unicamente per le seguenti finalità: a)valutare i passeggeri prima dell'arrivo previsto nello Stato membro o della partenza prevista dallo Stato membro per identificare quelli da sottoporre a ulteriore verifica da parte delle autorità competenti di cui all'articolo 7 e, se del caso, da parte di Europol, a norma dell'articolo 10, in considerazione del fatto che gli stessi potrebbero essere implicati in reati di terrorismo o in reati gravi; b)rispondere, caso per caso, a una richiesta debitamente motivata e basata su motivi sufficienti da parte delle autorità competenti di trasmettere e trattare dati PNR in casi specifici a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, e di comunicare i risultati di tale trattamento alle stesse autorità competenti o, se del caso, a Europol; e c)analizzare i dati PNR per aggiornare i criteri esistenti o definire nuovi criteri da usare nelle valutazioni effettuate ai sensi del paragrafo 3, lettera b), al fine di identificare le persone che potrebbero essere implicate in reati di terrorismo o in reati gravi. 3. Nell'effettuare la valutazione di cui al paragrafo		

2, lettera a), l'UIP può: a)confrontare i dati PNR rispetto a banche dati pertinenti a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, comprese le banche dati riguardanti persone o oggetti ricercati o segnalati, conformemente alle norme dell'Unione, internazionali e nazionali applicabili a tali banche dati; o b)trattare i dati PNR sulla base di criteri prestabiliti. 4. Ogni valutazione dei passeggeri secondo criteri prestabiliti di cui al paragrafo 3, lettera b), prima dell'arrivo previsto nello Stato membro o della partenza prevista dallo Stato membro, è effettuata in modo non discriminatorio. Tali criteri prestabiliti devono essere mirati, proporzionati e specifici. Gli Stati membri assicurano che detti criteri siano stabiliti dall'UIP e periodicamente rivisti in cooperazione con le autorità competenti di cui all'articolo 7. Detti criteri non sono in alcun caso basati 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. 5. Gli Stati membri provvedono affinché i riscontri positivi a seguito del		

trattamento automatizzato dei dati PNR effettuato a norma del paragrafo 2, lettera a), siano singolarmente sottoposti a un esame non automatizzato per verificare se sia necessario un intervento dell'autorità competente di cui all'articolo 7 conformemente al diritto nazionale. 6. L'UIP di uno Stato membro trasmette i dati PNR dei passeggeri identificati conformemente al paragrafo 2, lettera a), o il risultato del trattamento di tali dati, per ulteriore verifica, alle autorità competenti di cui all'articolo 7 dello stesso Stato membro. Tali trasferimenti sono effettuati solo caso per caso e, in caso di trattamento automatizzato dei dati PNR, dopo l'esame individuale non automatizzato. 7. Gli Stati membri assicurano che il responsabile della protezione dei dati abbia accesso a tutti i dati trattati dall'UIP. Se ritiene che il trattamento dei dati non sia stato lecito, il responsabile della protezione dei dati può rinviare la questione all'autorità nazionale di controllo. 8. La conservazione, il trattamento e l'analisi dei dati PNR da parte dell'UIP sono effettuati esclusivamente in un luogo o in luoghi sicuri all'interno del territorio degli Stati membri. 9. Le conseguenze delle		

valutazioni dei passeggeri di cui al paragrafo 2, lettera a), del presente articolo non pregiudicano il diritto delle persone che godono del diritto di libera circolazione dell'Unione di entrare nel territorio dello Stato membro interessato secondo quanto previsto dalla direttiva 2004/38/CE del Parlamento europeo e del Consiglio. Inoltre, se le valutazione sono effettuate in relazione a voli intra-UE tra Stati membri cui si applica il regolamento (CE) n. 562/2006 del Parlamento europeo e del Consiglio, le conseguenze di tali valutazioni devono rispettare tale regolamento.		
Articolo 7 Autorità competenti 1. Ciascuno Stato membro adotta l'elenco delle autorità competenti autorizzate a chiedere o ricevere dalle UIP i dati PNR o i risultati del loro trattamento ai fini di un'ulteriore verifica delle informazioni o di interventi appropriati per prevenire, accertare, indagare e perseguire reati di terrorismo o reati gravi. 2. Le autorità di cui al paragrafo 1 sono le autorità responsabili della prevenzione, dell'accertamento, dell'indagine o del perseguimento dei reati di terrorismo o dei reati gravi. 3. Ai fini dell'articolo 9, paragrafo 3, entro il 25 maggio 2017 ciascuno Stato membro		L'articolo 7 della direttiva prevede che ogni Stato membro stabilisca quali siano le autorità autorizzate a chiedere o ricevere dalle UIP i dati PNR o i risultati del loro trattamento. L'articolo della direttiva è ripreso dagli articoli 2, comma 2, 12 e 16 dello schema di decreto.

notifica alla Commissione l'elenco delle proprie autorità competenti e può modificare la sua notifica in qualsiasi momento. La Commissione pubblica la notifica e le eventuali modifiche della stessa nella Gazzetta ufficiale dell'Unione europea. 4. Le autorità competenti degli Stati membri possono sottoporre a ulteriore trattamento i dati PNR e i risultati del loro trattamento ricevuti dall'UIP unicamente al fine specifico di prevenire, accertare, indagare o perseguire reati di terrorismo o reati gravi. 5. Il paragrafo 4 non pregiudica le competenze delle autorità di contrasto e giudiziarie nazionali qualora siano individuati altri reati o indizi di reato durante l'azione di contrasto determinata da tale trattamento. 6. Le autorità competenti non devono adottare decisioni che comportino conseguenze giuridiche negative per l'interessato, o lo danneggino in modo significativo, soltanto sulla base del trattamento automatizzato dei dati PNR. Tali decisioni non devono essere adottate sulla base dell'origine razziale o etnica, delle opinioni politiche, della religione o delle convinzioni filosofiche, dell'appartenenza sindacale, dello stato di salute, della vita sessuale o dell'orientamento sessuale dell'interessato.		

Articolo 8 Obblighi dei vettori aerei riguardanti i trasferimenti di dati 1. Gli Stati membri adottano i necessari provvedimenti affinché i vettori aerei trasferiscano, attraverso il «metodo push», i dati PNR elencati nell'allegato I, a condizione che abbiano già raccolto tali dati nel normale svolgimento della loro attività, alla banca dati dell'UIP dello Stato membro nel cui territorio atterra o dal cui territorio parte il volo. Qualora il volo sia operato in code-sharing da uno o più vettori aerei, l'obbligo di trasferire i dati PNR di tutti i passeggeri del volo spetta al vettore aereo che opera il volo. Qualora un volo extra-UE faccia uno o più scali negli aeroporti degli Stati membri, i vettori aerei trasferiscono i dati PNR di tutti i passeggeri alle UIP di tutti gli Stati membri interessati. Lo stesso vale qualora un volo intra-UE faccia uno o più scali negli aeroporti di diversi Stati membri, ma solo in relazione agli Stati membri che raccolgono i dati PNR dei voli intra-UE. 2. Nel caso in cui i vettori aerei abbiano raccolto le informazioni anticipate sui passeggeri (API) di cui all'allegato I, punto 18, ma non conservino tali dati con gli stessi mezzi tecnici di quelli per gli altri dati PNR, gli Stati	Decreto legislativo 2 agosto 2007, n. 144, recante l'attuazione della Direttiva 2004/82/CE, concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate (art. 3).	L'articolo 8 della direttiva stabilisce che gli Stati membri adottino i necessari provvedimenti per il trasferimento dei dati PNR da parte dei vettori aerei (artt. 4 e 5).

membri adottano le misure necessarie affinché i vettori aerei trasferiscano, attraverso il «metodo push», anche detti dati all'UIP dello Stato membro di cui al paragrafo 1. In caso di trasferimento, tutte le disposizioni della presente direttiva si applicano in relazione a tali dati API. 3. I vettori aerei trasferiscono i dati PNR elettronicamente utilizzando i protocolli comuni e i formati di dati supportati da adottare secondo la procedura d'esame di cui all'articolo 17, paragrafo 2, o, in caso di guasto tecnico, con altro mezzo appropriato che assicuri un adeguato livello di sicurezza dei dati, conformemente alle seguenti condizioni: a)da 24 a 48 ore prima dell'ora prevista di partenza del volo; e b)immediatamente dopo la chiusura del volo, vale a dire una volta che i passeggeri sono saliti a bordo dell'aeromobile pronto per la partenza e non è più possibile l'imbarco o lo sbarco di passeggeri. 4. Gli Stati membri consentono ai vettori aerei di limitare il trasferimento di cui al paragrafo 3, lettera b), agli aggiornamenti dei trasferimenti di cui alla lettera a) di detto paragrafo. 5. Quando l'accesso ai dati PNR è necessario per rispondere a una minaccia specifica e reale connessa a		

reati di terrorismo o a reati gravi, i vettori aerei, caso per caso, trasferiscono i dati PNR in momenti diversi da quelli di cui al paragrafo 3, su richiesta di un'UIP conformemente al diritto nazionale.		
Articolo 9 Scambio di informazioni tra Stati membri 1. Gli Stati membri provvedono affinché, per quanto riguarda le persone identificate da un'UIP a norma dell'articolo 6, paragrafo 2, questa trasmetta tutti i dati PNR pertinenti e necessari o i risultati del loro trattamento alle corrispondenti UIP degli altri Stati membri. Le UIP degli Stati membri destinatari trasmettono, ai sensi dell'articolo 6, paragrafo 6, le informazioni ricevute alle rispettive autorità competenti. 2. L'UIP di uno Stato membro è autorizzata a chiedere, se necessario, all'UIP di qualsiasi altro Stato membro di trasmetterle i dati PNR conservati nella sua banca dati e che non sono stati ancora resi anonimi mediante mascheratura degli elementi dei dati a norma dell'articolo 12, paragrafo 2, e, se necessario, anche i risultati di qualsiasi trattamento di tali dati, se è già stato effettuato ai sensi dell'articolo 6, paragrafo 2, lettera a). Tale richiesta deve essere debitamente motivata. Può riguardare uno		La disposizione della direttiva disciplina lo scambio di informazioni tra gli Stati membri. L'articolo della direttiva è ripreso dagli articoli 13, 14, 15 16 e 17 dello schema di decreto.

o più elementi di dati combinati fra loro, secondo quanto ritenga necessario l'UIP richiedente in relazione a un caso specifico di prevenzione, accertamento, indagine o azione penale nei confronti di reati di terrorismo o di reati gravi. L'UIP comunica le informazioni richieste appena possibile. Nel caso in cui i dati richiesti siano stati resi anonimi mediante mascheratura degli elementi dei dati a norma dell'articolo 12, paragrafo 2, l'UIP trasmette i dati PNR integrali solo se è ragionevolmente ritenuto necessario ai fini dell'articolo 6, paragrafo 2, lettera b), e solo se autorizzata in tal senso da un'autorità di cui all'articolo 12, paragrafo 3, lettera b). 3. Le autorità competenti di uno Stato membro hanno facoltà di chiedere direttamente all'UIP di qualsiasi altro Stato membro di trasmettere loro i dati PNR conservati nella sua banca dati solo se necessario in situazioni di emergenza e alle condizioni previste al paragrafo 2. Le richieste delle autorità competenti devono essere motivate. Una copia della richiesta è sempre trasmessa all'UIP dello Stato membro richiedente. In tutti gli altri casi, le autorità competenti inoltrano le richieste tramite l'UIP del proprio Stato membro. 4. In circostanze eccezionali, se è necessario accedere a dati		

PNR per rispondere a una minaccia specifica e reale connessa a reati di terrorismo o reati gravi, l'UIP di uno Stato membro è autorizzata a chiedere all'UIP di un altro Stato membro di ottenere dati PNR ai sensi dell'articolo 8, paragrafo 5, e di trasmettere tali dati all'UIP richiedente. 5. Lo scambio di informazioni ai sensi del presente articolo può avvenire tramite qualsiasi canale esistente di cooperazione tra le autorità competenti degli Stati membri. La lingua utilizzata per la richiesta e lo scambio di informazioni è quella applicabile al canale utilizzato. Nell'effettuare le notifiche a norma dell'articolo 4, paragrafo 5, gli Stati membri comunicano alla Commissione anche gli estremi dei punti di contatto cui possono essere trasmesse le richieste in casi di emergenza. La Commissione comunica tali estremi agli Stati membri.		
Articolo 10 Condizioni per l'accesso di Europol ai dati PNR 1. Europol ha il diritto di chiedere i dati PNR o i risultati del trattamento di tali dati alle UIP degli Stati membri entro i limiti delle sue competenze e per l'adempimento dei suoi compiti. 2. Europol, per il tramite dell'unità nazionale Europol, può presentare, caso per caso,		L'articolo 10 della direttiva stabilisce le condizioni e le modalità per l'accesso di Europol ai dati PNR. L'articolo 10 della direttiva è disciplinato dall'articolo 18 dello schema di decreto.

all'UIP di uno Stato membro una richiesta elettronica e debitamente motivata di trasmissione di dati PNR o dei risultati del trattamento di tali dati. Europol può presentare tale richiesta qualora ciò si riveli strettamente necessario per sostenere e rafforzare l'azione degli Stati membri volta a prevenire, accertare o indagare uno specifico reato di terrorismo o reato grave, nella misura in cui si tratti di un reato di competenza di Europol conformemente alla decisione 2009/371/GAI. Detta richiesta espone i ragionevoli motivi in base ai quali Europol ritiene che la trasmissione dei dati PNR o dei risultati del trattamento di tali dati contribuisca significativamente alla prevenzione, all'accertamento o all'indagine nei confronti del reato in questione. 3. Europol informa il responsabile della protezione dei dati nominato a norma dell'articolo 28 della decisione 2009/371/GAI di qualsiasi scambio di informazioni ai sensi del presente articolo. 4. Lo scambio di informazioni ai sensi del presente articolo avviene tramite l'applicazione SIENA e conformemente alla decisione 2009/371/GAI. La lingua utilizzata per la richiesta e lo scambio di informazioni è quella applicabile a SIENA.		
Articolo 11 Trasferimento dei dati a paesi		L'articolo della direttiva definisce i presupposti per la trasmissione dei dati PNR e dei

terzi 1. Uno Stato membro può trasferire a un paese terzo i dati PNR nonché i risultati del trattamento di tali dati che sono conservati dall'UIP conformemente all'articolo 12 soltanto caso per caso e se: a) ricorrono le condizioni di cui all'articolo 13 della decisione quadro 2008/977/GAI; b) il trasferimento è necessario per le finalità di cui all'articolo 1, paragrafo 2, della presente direttiva; c) il paese terzo accetta di trasferire i dati a un altro paese terzo soltanto se il trasferimento è strettamente necessario per le finalità di cui all'articolo 1, paragrafo 2, della presente direttiva e soltanto previa autorizzazione esplicita di tale Stato membro; e d) sono rispettate le stesse condizioni di cui all'articolo 9, paragrafo 2. 2. Nonostante l'articolo 13, paragrafo 2, della decisione 2008/977/GAI, i trasferimenti di dati PNR senza consenso preliminare dello Stato membro dal quale sono stati ottenuti i dati sono autorizzati in circostanze eccezionali soltanto se: a) tali trasferimenti sono indispensabili per rispondere a una minaccia specifica e reale connessa a reati di terrorismo o reati gravi in uno Stato membro o un paese terzo; e b) il consenso preliminare non può essere ottenuto in tempo utile.		risultati del loro trattamento ai Paesi terzi. L'articolo 19 dello schema del decreto riproduce fedelmente la disciplina dettata dalla Direttiva PNR, arricchendola, tuttavia, di una necessaria precisazione: il trasferimento deve essere sì effettuato in presenza dei predetti presupposti, ma deve altresì fondarsi su un preventivo accordo appositamente stipulato tra lo Stato italiano e il Paese terzo interessato.

L'autorità responsabile di dare il consenso è informata senza indugio e il trasferimento è debitamente registrato e soggetto a verifica a posteriori. 3. Gli Stati membri trasferiscono i dati PNR alle autorità competenti di paesi terzi soltanto a condizioni conformi alla presente direttiva e soltanto previo accertamento che l'uso che intendono farne i destinatari è conforme alle condizioni e garanzie previste dalla presente direttiva. 4. Il responsabile della protezione dei dati dell'UIP dello Stato membro che ha trasferito i dati PNR è informato ogni volta che uno Stato membro trasferisce dati PNR a norma del presente articolo.		
Articolo 12 Periodo di conservazione dei dati e anonimato 1. Gli Stati membri provvedono affinché i dati PNR trasmessi dai vettori aerei all'UIP siano da questa conservati in una banca dati per un periodo di cinque anni dal trasferimento all'UIP dello Stato membro dal cui territorio parte o nel cui territorio atterra il volo. 2. Allo scadere del periodo di sei mesi dal trasferimento dei dati PNR di cui al paragrafo 1, tutti i dati PNR sono resi anonimi mediante	Decreto legislativo 2 agosto 2007, n. 144, recante l'attuazione della Direttiva 2004/82/CE, concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate (art. 4).	L'articolo della direttiva stabilisce il periodo massimo di conservazione dei dati, nonché il periodo oltre il quale detti dati devono essere resi anonimi. Per quanto disciplinato dal presente articolo si veda l'articolo 10 del decreto.

mascheratura dei seguenti elementi che potrebbero servire a identificare direttamente il passeggero cui i dati PNR si riferiscono: a) il nome o i nomi, compresi i nomi di altri passeggeri figuranti nel PNR e il numero di viaggiatori che viaggiano insieme figurante nel PNR; b) l'indirizzo e gli estremi; c) informazioni su tutte le modalità di pagamento, compreso l'indirizzo di fatturazione, nella misura in cui contenga informazioni che potrebbero servire a identificare direttamente il passeggero cui si riferiscono i dati PNR o altre persone; d) informazioni sui viaggiatori abituali («Frequent flyer»); e) osservazioni generali contenenti informazioni che potrebbero servire a identificare direttamente il passeggero cui si riferiscono i dati PNR; e f) i dati API eventualmente raccolti. 3. Allo scadere del periodo di sei mesi di cui al paragrafo 2, la comunicazione dei dati PNR integrali è consentita solo se: a) è ragionevolmente ritenuta necessaria ai fini dell'articolo 6, paragrafo 2, lettera b); e b) è approvata da: i) un'autorità giudiziaria; o ii) un'altra autorità nazionale competente ai sensi del diritto nazionale per verificare se sono soddisfatte		

le condizioni per la comunicazione, fatti salvi l'informazione e l'esame a posteriori del responsabile della protezione dei dati dell'UIP. 4. Gli Stati membri provvedono affinché i dati PNR siano cancellati in via definitiva allo scadere del periodo di cui al paragrafo 1. Questo obbligo non incide sui casi in cui dati PNR specifici sono stati trasferiti a un'autorità competente e sono usati nell'ambito di un caso specifico a fini di prevenzione, accertamento, indagine e azione penale dei reati di terrorismo o reati gravi, nel qual caso la loro conservazione presso l'autorità competente è disciplinata dal diritto nazionale. 5. I risultati del trattamento di cui all'articolo 6, paragrafo 2, lettera a), sono conservati presso l'UIP soltanto per il tempo necessario a informare di un riscontro positivo le autorità competenti e, conformemente all'articolo 9, paragrafo 1, a informare di un riscontro positivo le UIP degli altri Stati membri. Il risultato di un trattamento automatizzato, anche qualora risulti negativo a seguito dell'esame individuale non automatizzato di cui all'articolo 6, paragrafo 5, può comunque essere memorizzato in modo da evitare futuri «falsi» riscontri positivi fino a che i dati di riferimento non sono cancellati a norma del		

paragrafo 4 del presente articolo.		
Articolo 13 Protezione dei dati personali 1. Ciascuno Stato membro dispone che, in relazione a qualsiasi trattamento di dati personali a norma della presente direttiva, ogni passeggero goda di un diritto di protezione dei dati personali, dei diritti di accesso, di rettifica, cancellazione e limitazione, così come dei diritti a compensazione e di proporre un ricorso giurisdizionale identici a quelli previsti dal diritto dell'Unione e nazionale e in attuazione degli articoli 17, 18, 19 e 20 della decisione quadro 2008/977/GAI. Si applicano pertanto le disposizioni di tali articoli. 2. Ciascuno Stato membro dispone che le norme nazionali di attuazione degli articoli 21 e 22 della decisione quadro 2008/977/GAI riguardanti la riservatezza del trattamento e la sicurezza dei dati si applichino anche a qualsiasi trattamento di dati personali effettuato a norma della presente direttiva. 3. La presente direttiva fa salva l'applicabilità della direttiva 95/46/CE del Parlamento europeo e del Consiglio (13) al trattamento di dati personali da parte dei vettori aerei, in particolare i loro obblighi relativi all'adozione di adeguate misure tecniche e	D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali); Legge 1 aprile 1981, n. 121, articolo 10, commi 3, 4 e 5.	L'articolo della direttiva prevede che ogni Stato membro deve assicurare: - la protezione dei dati personali; - il divieto del trattamento dei dati PNR idonei 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 sessuali dell'interessato; - la conservazione da parte dell'UIP della documentazione relativa a tutti i sistemi e tutte le procedure di trattamento; - l'adozione da parte della UIP di misure e procedure tecniche e organizzative per garantire un livello elevato di sicurezza che sia appropriato ai rischi che il trattamento comporta e alla natura dei dati PNR; - la tenuta dei registri da parte dell'UIP per determinate operazioni di trattamento, nonché la loro conservazione. L'articolo della direttiva è ripreso dagli articoli 22 e 23 dello schema normativo.

organizzative a tutela della sicurezza e della riservatezza dei dati personali. 4. Gli Stati membri vietano il trattamento dei dati PNR che riveli 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 sessuali dell'interessato. Qualora l'UIP riceva dati PNR che rivelano tali informazioni, questi sono cancellati immediatamente. 5. Gli Stati membri provvedono affinché l'UIP conservi la documentazione relativa a tutti i sistemi e tutte le procedure di trattamento sotto la propria responsabilità. Tale documentazione comprende almeno: a) il nome e le coordinate di contatto dell'organizzazione e del personale dell'UIP incaricati del trattamento dei dati PNR e i diversi livelli di autorizzazione d'accesso; b) le richieste delle autorità competenti e delle UIP di altri Stati membri; c) tutte le richieste e i trasferimenti di dati PNR verso un paese terzo. Su richiesta, l'UIP mette a disposizione dell'autorità nazionale di controllo tutta la documentazione disponibile. 6. Gli Stati membri provvedono affinché l'UIP tenga registri almeno delle seguenti operazioni di trattamento: raccolta,		

consultazione, comunicazione e cancellazione. I registri delle consultazioni e comunicazioni indicano, in particolare, la finalità, la data e l'ora dell'operazione e, nella misura del possibile, l'identità della persona che ha consultato o comunicato i dati PNR, nonché l'identità 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. Su richiesta, l'UIP mette i registri a disposizione dell'autorità nazionale di controllo. Tali registri sono conservati per un periodo di cinque anni. 7. Gli Stati membri provvedono affinché l'UIP metta in atto adeguate misure e procedure tecniche e organizzative per garantire un livello elevato di sicurezza che sia appropriato ai rischi che il trattamento comporta e alla natura dei dati PNR. 8. Gli Stati membri provvedono affinché, quando una violazione di dati personali è suscettibile di determinare un rischio elevato per la protezione dei dati personali o di incidere negativamente sulla vita privata dell'interessato, l'UIP comunichi la violazione all'interessato e all'autorità nazionale di controllo senza ingiustificato ritardo.		
Articolo 14 Sanzioni	Decreto legislativo 2 agosto 2007, n. 144, recante l'attuazione della Direttiva	L'articolo 14 della direttiva prevede l'applicazione di sanzioni per la violazione delle

Gli Stati membri stabiliscono le sanzioni applicabili alle violazioni delle disposizioni nazionali adottate a norma della presente direttiva e adottano le misure necessarie per garantirne l'attuazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive. In particolare, gli Stati membri stabiliscono le norme relative alle sanzioni, anche pecuniarie, a carico dei vettori aerei che non trasmettono i dati, come previsto dall'articolo 8, o non li trasmettono nel formato richiesto. Le sanzioni previste devono essere effettive, proporzionate e dissuasive.	2004/82/CE, concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate (art. 5 e 6).	disposizioni nazionali eventualmente adottate individuando le specifiche, stabilendo altresì, che debbano essere effettive, proporzionate e dissuasive. L'articolo 24 dello schema di decreto stabilisce idonee sanzioni amministrative e le autorità competenti a irrogarle.
Articolo 15 Autorità nazionale di controllo 1. Ogni Stato membro dispone che l'autorità nazionale di controllo di cui all'articolo 25 della decisione quadro 2008/977/GAI sia incaricata di fornire consulenza e di esercitare la sorveglianza, nel suo territorio, riguardo all'applicazione delle disposizioni adottate dagli Stati membri conformemente alla presente direttiva. Si applica l'articolo 25 della decisione quadro 2008/977/GAI. 2. Tali autorità nazionali di controllo svolgono le attività di cui al paragrafo 1, così da tutelare i diritti fondamentali	D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali)	L'articolo della direttiva affida all'Autorità nazionale di controllo l'incarico di fornire consulenza e di esercitare la sorveglianza, nel suo territorio, riguardo all'applicazione delle disposizioni adottate dagli Stati membri. L'articolo 20 dello schema di decreto individua la suddetta Autorità nazionale nel Garante per la protezione dei dati personali e attribuisce espressamente allo stesso l'esercizio della funzione di controllo con le modalità previste dal Codice in materia di protezione dei dati personali.

in relazione al trattamento dei dati personali. 3. Ciascuna autorità nazionale di controllo: a) tratta i reclami presentati dagli interessati, svolge le relative indagini e informa gli interessati, entro un termine ragionevole, dello stato e dell'esito del reclamo; b) verifica la liceità del trattamento dei dati, svolge indagini, ispezioni e audit conformemente al diritto nazionale, di propria iniziativa o a seguito di un reclamo di cui alla lettera a). 4. Ciascuna autorità nazionale di controllo, su richiesta, consiglia l'interessato in merito all'esercizio dei diritti derivanti dalle disposizioni adottate conformemente alla presente direttiva.		
Articolo 16 Protocolli comuni e formati di dati supportati 1. Tutti i trasferimenti di dati PNR dai vettori aerei alle UIP ai fini della presente direttiva sono effettuati con un mezzo elettronico che offra sufficienti garanzie rispetto alle misure di sicurezza tecniche e alle misure organizzative relative ai trattamenti da effettuare. In caso di guasto tecnico, i dati PNR possono essere trasferiti con altro mezzo appropriato, purché sia mantenuto lo stesso livello di sicurezza e sia pienamente rispettato il diritto dell'Unione in materia di protezione dei dati.		L'articolo 16 della direttiva, stabilisce l'adozione di protocolli comuni e di formati di dati supportati, nonché il trasferimento di dati PNR dai vettori aerei alle UIP elettronicamente e con metodi sicuri, conformi a tali protocolli comuni. La presente disposizione è ripresa dall'articolo 5, commi 2 e 3 dell'emanando decreto.

2. Un anno dopo la data di prima adozione da parte della Commissione dei protocolli comuni e dei formati di dati supportati a norma del paragrafo 3, tutti i trasferimenti di dati PNR dai vettori aerei alle UIP ai fini della presente direttiva sono effettuati elettronicamente e con metodi sicuri conformi a tali protocolli comuni. Tali protocolli sono identici per tutti i trasferimenti, che garantiscano la sicurezza dei dati PNR durante il trasferimento. I dati PNR sono trasferiti in un formato di dati supportato che ne garantisca la leggibilità a tutti gli interessati. Tutti i vettori aerei hanno l'obbligo di scegliere e notificare all'UIP il protocollo comune e il formato di dati che intendono usare per i loro trasferimenti. 3. La Commissione stabilisce l'elenco dei protocolli comuni e dei formati di dati supportati e, se necessario, lo adegua mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 17, paragrafo 2. 4. Il paragrafo 1 si applica, finché non sono disponibili i protocolli comuni e i formati di dati supportati di cui ai paragrafi 2 e 3. 5. Entro un anno dall'adozione dei protocolli comuni e dei formati di dati supportati di cui		

al paragrafo 2, ciascuno Stato membro provvede affinché siano adottate le necessarie misure tecniche per poter usare tali protocolli comuni e i formati di dati.		
Articolo 17 Procedura di comitato 1. La Commissione è assistita da un comitato. Tale comitato è un comitato ai sensi del regolamento (UE) n. 182/2011. 2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011. Nel caso in cui il comitato non esprima alcun parere, la Commissione non adotta il progetto di atto di esecuzione e si applica l'articolo 5, paragrafo 4, terzo comma, del regolamento (UE) n. 182/2011.		La norma non necessita di attuazione.
Articolo 18 Recepimento 1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 25 maggio 2018. Essi ne informano immediatamente la Commissione. Le disposizioni adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le		L'articolo 18 della direttiva fissa al 25 maggio 2018 il termine massimo per il suo recepimento.

modalità del riferimento sono stabilite dagli Stati membri. 2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni fondamentali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.		
Articolo 19 Riesame 1. Sulla scorta delle informazioni fornite dagli Stati membri, tra cui le statistiche di cui all'articolo 20, paragrafo 2, la Commissione procede a un riesame di tutti gli elementi della presente direttiva e sottopone e inoltra una relazione al Parlamento europeo e al Consiglio entro il 25 maggio 2020. 2. Nell'ambito di tale riesame, la Commissione presta particolare attenzione: a) al rispetto del livello applicabile di protezione dei dati personali; b) alla necessità e alla proporzionalità della raccolta e del trattamento dei dati PNR per ciascuna delle finalità di cui alla presente direttiva; c) alla durata del periodo di conservazione dei dati; d) all'efficacia dello scambio di informazioni fra gli Stati membri; e e) alla qualità delle valutazioni anche con riferimento alle statistiche elaborate a norma dell'articolo 20.		L'articolo della direttiva stabilisce che, sulla scorta delle informazioni fornite dagli Stati membri, la Commissione proceda a riesaminare tutti gli elementi trattati e a predisporre un'apposita relazione da inviare al Parlamento europeo e al Consiglio entro il 25 maggio 2020. La norma non necessita di attuazione.

3. La relazione di cui al paragrafo 1 comprende altresì un riesame della necessità, della proporzionalità e dell'efficacia dell'inclusione, nell'ambito di applicazione della presente direttiva, della raccolta obbligatoria e del trasferimento dei dati PNR riguardanti tutti i voli intra-UE o i voli intra-UE selezionati. La Commissione prende in considerazione l'esperienza maturata dagli Stati membri, in particolare da quelli che attuano questa direttiva ai voli intra-UE a norma dell'articolo 2. La relazione esamina anche la necessità di inserire operatori economici diversi dai vettori aerei, come le agenzie di viaggio e gli operatori turistici, che forniscono servizi connessi ai viaggi, fra cui la prenotazione di voli, nell'ambito di applicazione della presente direttiva. 4. Se del caso, alla luce del riesame condotto a norma del presente articolo, la Commissione presenta al Parlamento europeo e al Consiglio una proposta legislativa intesa a modificare la presente direttiva.		
Articolo 20 Statistiche 1. Gli Stati membri forniscono annualmente alla Commissione una serie di statistiche sui dati PNR trasmessi alle UIP. Tali statistiche non contengono dati personali.		L'articolo della direttiva stabilisce che annualmente gli Stati membri forniscano alla Commissione europea elaborazioni statistiche concernenti i dati PNR trasmessi all'UIP nazionale. L'articolo della direttiva è trasposto nell'articolo 25 del decreto.

2. Le statistiche indicano quanto meno: a) il numero totale di passeggeri i cui dati PNR sono stati raccolti e scambiati; b) il numero di passeggeri identificati a fini di ulteriore esame.		
Articolo 21 Relazione con altri strumenti 1. Gli Stati membri possono continuare ad applicare tra loro gli accordi o le intese bilaterali o multilaterali sullo scambio di informazioni tra autorità competenti in vigore il entro il 24 maggio 2016, purché siano compatibili con quest'ultima. 2. La presente direttiva fa salva l'applicabilità della direttiva 95/46/CE al trattamento dei dati personali da parte dei vettori aerei. 3. La presente direttiva non pregiudica gli obblighi e impegni degli Stati membri o dell'Unione derivanti da accordi bilaterali o multilaterali conclusi con paesi terzi.		La disposizione stabilisce che gli Stati membri possano continuare ad applicare tra loro gli accordi o le intese bilaterali o multilaterali sullo scambio di informazioni. Lo schema riprende tale disposizione nell'art. 1, comma 3.
Articolo 22 Entrata in vigore La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Gli Stati membri sono destinatari della presente direttiva conformemente ai		L'articolo fissa l'entrata in vigore della direttiva.

trattati.		

RELAZIONE TECNICO NORMATIVA

Amministrazioni proponenti:Presidenza del Consiglio dei Ministri e dei Ministeri dell'interno e della giustizia, di concerto con i Ministeri della difesa e dell'economia e delle finanze.

Titolo: Schema di decreto legislativo recante: "Attuazione della direttiva 27 aprile 2016, n 2016/681/UE del Parlamento Europeo e del Consiglio sull'uso dei dati del codice di prenotazione (PNR) ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.".

Indicazione del referente dell'amministrazione proponente: Dr. Paolo Corritore, Dirigente Ufficio Affari Legislativi e Relazioni parlamentari - Ufficio V – Pubblica Sicurezza (Tel. 06-46547061 – 06/46548152 – 06/46538308)

PARTE I. ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) OBIETTIVI E NECESSITÀ DELL'INTERVENTO NORMATIVO. COERENZA CON IL PROGRAMMA DI GOVERNO.

Con lo schema di decreto legislativo in esame si dà attuazione alla delega legislativa conferita al Governo dagli articoli 1 e 12 della legge 25 ottobre 2017, n. 163 (*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017*) che stabilisce, fra l'altro, che nell'ordinamento interno venga recepita la direttiva UE 2016/681 sull'uso dei dati del codice di prenotazione (PNR). Con il presente provvedimento si provvede a dotare il nostro Paese, così da "allinearlo" ad altri Stati membri dell'Unione Europea, di un ulteriore strumento nelle attività di prevenzione e di contrasto dei reati di terrorismo e di altri reati gravi. Il decreto disciplina, contestualmente, l'obbligo di trasmissione delle informazioni introdotto dalla direttiva 2004/82/CE del 29 aprile 2004, (di seguito, «Direttiva API»), assorbendo la relativa normativa di attuazione e disponendo l'abrogazione della stessa dal momento dell'entrata in vigore dei propri provvedimenti attuativi.

Ciò in quanto, l'eventuale coesistenza di due provvedimenti attuativi autonomi assoggetterebbe l'obbligo di trasmissione dei dati API a fonti normative diverse, creando una situazione di incertezza, con il rischio di una duplicazione degli adempimenti per i vettori aerei, a causa della presenza di distinti sistemi informativi, con conseguenti ripercussioni per gli interessati, anche sotto il profilo della possibile lesione del diritto di protezione dei dati personali.

Il descritto processo di assorbimento, invece, appare coerente con il principio direttivo della massima semplificazione dei procedimenti, enunciato dall'articolo 32 della Legge 24 dicembre 2012, n. 234. Si realizza, pertanto, un intervento di semplificazione e razionalizzazione delle procedure, attraverso l'introduzione di un meccanismo di condivisione delle informazioni, finalizzato al rafforzamento della tutela della sicurezza all'interno dello spazio comune europeo.

2) ANALISI DEL QUADRO NORMATIVO NAZIONALE.

Il quadro normativo di riferimento è costituito dai provvedimenti di seguito elencati:

- 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 2016-2017*» (artt. 1 e 12);
- decreto legislativo 23 aprile 2015, n. 54, recante «*Attuazione della decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006*»;
- decreto legislativo 6 settembre 2011, n. 159 recante: "*Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia*";
- legge 3 agosto 2007, n. 124, recante "*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*
- decreto legislativo 2 agosto 2007, n. 144 recante «*Attuazione della direttiva 2004/82/CE concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate*»;
- 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;
- Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;
- decreto legislativo 25 luglio 1998, n. 286, recante «*Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero*»;
- decreto legislativo 25 luglio 1997, n. 250, istitutivo dell'Ente nazionale per l'aviazione civile (ENAC);
- 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;
- decreto del Presidente della Repubblica 3 maggio 1982, n. 378, recante «*Approvazione del regolamento concernente le procedure di raccolta, accesso, comunicazione, correzione, cancellazione ed integrazione dei dati e delle informazioni, registrati negli archivi magnetici del centro elaborazione dati di cui all'art. 8 della legge 1° aprile 1981, n. 121*»:
- legge 24 novembre 1981, n. 689, recante modifiche al sistema penale;
- legge 1 aprile 1981, n, 121, recante «*Nuovo ordinamento dell'amministrazione della pubblica sicurezza*»;
- regio decreto 30 marzo 1942, n. 327, recante l'approvazione del testo definitivo del Codice della navigazione, e successive modifiche ed integrazioni.

3) INCIDENZA DELLE NORME PROPOSTE SULLE LEGGI E I REGOLAMENTI VIGENTI.
Lo schema di decreto in esame, finalizzato al recepimento dei contenuti della direttiva UE/2016/681 sull'uso del codice di prenotazione (PNR), tiene conto del fatto che il nostro ordinamento giuridico ha già recepito con il decreto legislativo 2 agosto 2007, n. 144, la direttiva 2004/82/CE, introduttiva dell'obbligo per i vettori aerei di comunicare, ai competenti uffici di polizia di frontiera, talune informazioni relative alle persone trasportate nel territorio dello Stato (API). Peraltro, al fine di operare una semplificazione e razionalizzazione del sistema, anziché procedere all'istituzione di una ulteriore banca dati, in cui far confluire informazioni in parte "sovrapponibili" a quelle già contenute nella banca dati API, il provvedimento opera una *reductio ad unitatem* degli archivi informatici destinati a contenere i dati relativi ad API e PNR.
Pertanto, allorché entreranno in vigore i decreti attuativi del presente decreto legislativo, il decreto legislativo 2 agosto 2007, n. 144, verrà abrogato e cesserà di trovare applicazione.

4) ANALISI DELLA COMPATIBILITÀ DELL'INTERVENTO CON I PRINCIPI COSTITUZIONALI.
Il provvedimento non presenta profili di incompatibilità con i principi costituzionali ed è in linea coerente con l'articolo 11 della Costituzione.

5) ANALISI DELLE COMPATIBILITÀ DELL'INTERVENTO CON LE COMPETENZE E LE FUNZIONI DELLE REGIONI ORDINARIE E A STATUTO SPECIALE NONCHÉ DEGLI ENTI LOCALI.
Lo schema di decreto legislativo non presenta aspetti di interferenza o di incompatibilità con le competenze costituzionali delle Regioni, incidendo su materia riservata alla competenza dello Stato (art. 117 Costituzione, lettere *a)* e *h)*.

6) VERIFICA DELLA COMPATIBILITÀ CON I PRINCIPI DI SUSSIDIARIETÀ, DIFFERENZIAZIONE ED ADEGUATEZZA SANCITI DALL'ARTICOLO 118, PRIMO COMMA, DELLA COSTITUZIONE.
Le disposizioni contenute nell'intervento esaminato sono compatibili e rispettano i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118 della Costituzione, in quanto non prevedono né determinano, anche solo in via indiretta, nuovi o più onerosi adempimenti a carico degli enti locali.

7) VERIFICA DELL'ASSENZA DI RILEGIFICAZIONI E DELLA PIENA UTILIZZAZIONE DELLE POSSIBILITÀ DI DELEGIFICAZIONE E DEGLI STRUMENTI DI SEMPLIFICAZIONE NORMATIVA.
Il decreto non contiene norme di rilegificazione. Sotto il profilo della semplificazione normativa, come detto, si è colta l'occasione per razionalizzare la materia optandosi, per la creazione di un'unica banca dati che contenga le informazioni API e PNR, tenuto anche conto del fatto che i dati API costituiscono un sottoinsieme dei dati PNR.

8) VERIFICA DELL'ESISTENZA DI PROGETTI DI LEGGE VERTENTI SU MATERIA ANALOGA ALL'ESAME DEL PARLAMENTO E RELATIVO STATO DELL'ITER.
Allo stato, non risultano pendenti in Parlamento proposte legislative di analogo contenuto.

9) INDICAZIONI DELLE LINEE PREVALENTI DELLA GIURISPRUDENZA OVVERO DELLA PENDENZA DI GIUDIZI DI COSTITUZIONALITÀ SUL MEDESIMO O ANALOGO OGGETTO.
Non si è a conoscenza di giudizi di costituzionalità pendenti nella specifica materia.

PARTE II. CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

10) ANALISI DELLA COMPATIBILITÀ DELL'INTERVENTO CON L'ORDINAMENTO COMUNITARIO.
Lo schema di decreto legislativo non presenta aspetti di interferenza o di incompatibilità con l'ordinamento europeo ed, anzi, attua nell'ordinamento interno le disposizioni contenute nella direttiva, completando il percorso di adeguamento della normativa nazionale al diritto europeo in materia.

11) VERIFICA DELL'ESISTENZA DI PROCEDURE DI INFRAZIONE DA PARTE DELLA COMMISSIONE EUROPEA SUL MEDESIMO O ANALOGO OGGETTO.
Non risultano procedimenti di infrazione sulle materie oggetto dell'intervento.

12) ANALISI DELLA COMPATIBILITÀ DELL'INTERVENTO CON GLI OBBLIGHI INTERNAZIONALI.
L'intervento è pienamente compatibile con gli obblighi internazionali e si pone in piena continuità con la necessità di adeguamento dell'ordinamento interno alle norme comunitarie.

13) INDICAZIONI DELLE LINEE PREVALENTI DELLA GIURISPRUDENZA OVVERO DELLA PENDENZA DI GIUDIZI INNANZI ALLA CORTE DI GIUSTIZIA DELLE COMUNITÀ EUROPEE SUL MEDESIMO O ANALOGO OGGETTO.
Non risultano giudizi pendenti innanzi alla Corte di giustizia.

14) INDICAZIONI DELLE LINEE PREVALENTI DELLA GIURISPRUDENZA OVVERO DELLA PENDENZA DI GIUDIZI INNANZI ALLA CORTE EUROPEA DEI DIRITTI DELL'UOMO SUL MEDESIMO O ANALOGO OGGETTO.
Non risultano indicazioni prevalenti di giurisprudenza della Corte europea del diritti dell'uomo o giudizi pendenti davanti alla stessa.

15) EVENTUALI INDICAZIONI SULLE LINEE PREVALENTI DELLA REGOLAMENTAZIONE SUL MEDESIMO OGGETTO DA PARTE DI ALTRI STATI MEMBRI DELL'UNIONE EUROPEA.
Non risultano particolari indicazioni di linee prevalenti della regolamentazione in altri Stati membri dell'Unione europea rilevanti ai fini degli interventi specifici in esame.

PARTE III. ELEMENTI DI QUALITA' SISTEMATICA E REDAZIONALE DEL TESTO

1) INDIVIDUAZIONE DELLE NUOVE DEFINIZIONI NORMATIVE INTRODOTTE DAL TESTO, DELLA LORO NECESSITÀ, DELLA COERENZA CON QUELLE GIÀ IN USO.
Lo schema di decreto in esame introduce la definizione di "dati PNR", relativa alle informazioni di viaggio di ciascun passeggero che utilizzi vettori aerei. Tale definizione risulta coerente con il linguaggio tecnico-giuridico di settore.

2) VERIFICA DELLA CORRETTEZZA DEI RIFERIMENTI NORMATIVI CONTENUTI NEL PROGETTO, CON PARTICOLARE RIGUARDO ALLE SUCCESSIVE MODIFICAZIONI ED INTEGRAZIONI SUBITE DAI MEDESIMI.
È stata verificata la correttezza e l'aggiornamento dei riferimenti normativi contenuti nel provvedimento.

3) RICORSO ALLA TECNICA DELLA NOVELLA LEGISLATIVA PER INTRODURRE MODIFICAZIONI ED INTEGRAZIONI A DISPOSIZIONI VIGENTI.
Lo schema di decreto in esame non fa ricorso alla tecnica della novella normativa.

4) INDIVIDUAZIONE DI EFFETTI ABROGATIVI IMPLICITI DI DISPOSIZIONI DELL'ATTO NORMATIVO E LORO TRADUZIONE IN NORME ABROGATIVE ESPRESSE NEL TESTO NORMATIVO.
Lo schema di decreto in esame non contiene norme da cui derivano abrogazioni implicite di altre disposizioni.

5) INDIVIDUAZIONE DI DISPOSIZIONI DELL'ATTO NORMATIVO AVENTI EFFETTO RETROATTIVO O DI REVIVISCENZA DI NORME PRECEDENTEMENTE ABROGATE O DI INTERPRETAZIONE AUTENTICA O DEROGATORIE RISPETTO ALLA NORMATIVA VIGENTE.
Lo schema di decreto in esame non contiene disposizioni aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

6) VERIFICA DELLA PRESENZA DI DELEGHE APERTE SUL MEDESIMO OGGETTO, ANCHE A CARATTERE INTEGRATIVO O CORRETTIVO.
Lo schema di decreto in esame non è attuativo di deleghe aperte sul medesimo oggetto.

7) INDICAZIONE DEGLI EVENTUALI ATTI SUCCESSIVI ATTUATIVI; VERIFICA DELLA CONGRUENZA DEI TERMINI PREVISTI PER LA LORO ADOZIONE.
Con uno o più decreti ministeriali di natura non regolamentare, da adottarsi 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, saranno disciplinate le modalità:

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 di mascheramento e cancellazione dei dati ai sensi dell'articolo 10;
d) di raffronto informatico dei dati PNR con quelli conservati nel Centro elaborazione dati 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 trasferimento delle informazioni, con strumenti informatici, dall'UIP nazionale alle autorità competenti nazionali;

f) di trasferimento dei dati PNR da parte dei vettori aerei;
g) di trattamento dei dati API da parte dei competenti Uffici incaricati dei controlli di polizia di frontiera.

8) VERIFICA DELLA PIENA UTILIZZAZIONE E DELL'AGGIORNAMENTO DI DATI E DI RIFERIMENTI STATISTICI ATTINENTI ALLA MATERIA OGGETTO DEL PROVVEDIMENTO, OVVERO INDICAZIONE DELLA NECESSITÀ DI COMMISSIONARE ALL'ISTITUTO NAZIONALE DI STATISTICA APPOSITE ELABORAZIONI STATISTICHE CON CORRELATA INDICAZIONE NELLA RELAZIONE ECONOMICO-FINANZIARIA DELLA SOSTENIBILITÀ DEI RELATIVI COSTI.

Lo schema di decreto in esame utilizza dati e riferimenti statistici in possesso del Ministero dell'interno.

Relazione tecnica

La presente nota tecnica è volta a valutare gli effetti finanziari derivanti dal provvedimento indicato in epigrafe, al fine di verificare il rispetto della clausola di invarianza di spesa stabilita dall'articolo 12, comma 2, della Legge di delegazione europea 2016-2017 (Legge 25 ottobre 2017, n. 163).

Il provvedimento è emanato ai sensi del citato articolo 12, il quale delega il Governo a adottare un decreto legislativo per l'attuazione della Direttiva 27 aprile 2016, n. 2016/681/UE del Parlamento europeo e del Consiglio 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 (nel prosieguo, «Direttiva PNR»), il cui termine di recepimento scade il 25 maggio 2018.

Prima di entrare nel merito delle disposizioni recate dal decreto, occorre premettere che la Direttiva PNR si prefigge l'obiettivo di rafforzare il sistema di sicurezza europeo tramite mirati controlli sui flussi di passeggeri aerei all'interno e all'esterno dell'Unione Europea.

Tali controlli si sviluppano attraverso l'analisi di determinate informazioni, piuttosto ampie e elencate specificamente nell'allegato I della Direttiva (nel prosieguo, «dati PNR»), che ciascun passeggero fornisce ai vettori aerei in fase di prenotazione del volo. Si tratta di un insieme di dati che consente un'attività di analisi di assoluto rilievo, finalizzata all'individuazione di passeggeri sospettati di essere implicati in reati di terrorismo o in altri reati gravi.

Il trattamento delle informazioni e le connesse attività saranno svolti dall'Unità d'informazione sui passeggeri (UIP) nazionale, ossia dall'unità appositamente istituita presso la Direzione Centrale della Polizia Criminale del Dipartimento della pubblica sicurezza del Ministero dell'Interno, ai fini dell'analisi dei dati PNR, per la quale si rinvia al prosieguo della trattazione (articolo 6).

Per l'effettuazione di tale attività di analisi è stato istituito apposito Sistema Informativo presso il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno, attraverso il quale i dati PNR vengono raccolti e trattati, ai sensi dell'**articolo 4** del presente decreto.

Il Sistema Informativo consente la contestuale gestione delle informazioni sui passeggeri acquisite ai sensi della Direttiva 29 aprile 2004, n. 2004/82/CE (nel prosieguo «dati API») ed è destinato quindi a sostituire, a completo regime, il Sistema informativo frontaliero *Border Control System* (BCS), attualmente utilizzato dagli Uffici incaricati dei controlli di polizia di frontiera per le finalità e alle condizioni previste dalla citata Direttiva (nel prosieguo, «Direttiva API»).

In particolare, la soluzione tecnica da realizzare si concretizza in una piattaforma informatica unitaria per garantire un'efficace, efficiente ed economica gestione dei dati PNR e dei dati API, da realizzare presso il Centro Elettronico Nazionale della Polizia di Stato di Napoli, con connessione al sito di *Disaster Recovery* presso il Centro Polifunzionale di Bari.

Ai fini dell'attuazione della Direttiva PNR, la Legge 11 dicembre 2016, n. 232, "Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019", all'articolo 1, comma 608, ha stanziato 5,5 milioni di euro per l'anno 2017, 16

milioni di euro per l'anno 2018 per la realizzazione della piattaforma informatica e 4,5 milioni di euro a decorrere dall'anno 2019 per la gestione e la manutenzione della stessa.

Le risorse previste dal predetto articolo 1, comma 608, sono state allocate sui seguenti capitoli di spesa:

- Cap. 7505 "Spese per la realizzazione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)" – parte capitale.
  Anno 2017 – euro 5.500.000
  Anno 2018 – euro 16.000.000
  Anno 2019 - 0
- Cap. 2563 "Spese per la gestione e la manutenzione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)" – parte corrente.
  Anno 2017 – 0
  Anno 2018 – 0
  Anno 2019 – euro 4.500.000.

La Legge 27 dicembre 2017, n. 205, "Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020" ha quindi disposto i seguenti stanziamenti:

- Cap. 7505 "Spese per la realizzazione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)"
  Anno 2018 – euro 16.000.000
  Anno 2019 – 0
  Anno 2020 - 0
- Cap. 2563 "Spese per la gestione e la manutenzione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)"
  Anno 2018 – 0
  Anno 2019 – euro 4.500.000
  Anno 2020 – euro 4.500.000.

Si soggiunge che, con la decisione di esecuzione del 18 settembre 2017, la Commissione europea ha reso disponibili ulteriori risorse sul Fondo Sicurezza Interno – Programma Nazionale dell'Italia (ISF) pari a euro 5.988.253, per il 50% di quota europea, ai fini della specifica attuazione della Direttiva (UE) 681/2016. Conseguentemente, tali risorse, unitamente a quelle di pari entità cofinanziate dall'Italia, hanno consentito di progettare la realizzazione di ulteriori funzioni necessarie ad elevare l'efficienza dell'infrastruttura tecnologica destinata al trattamento dei dati PNR e alle connesse attività dell'UIP nazionale.

Le accresciute disponibilità e una più puntuale definizione del quadro esigenziale emerso nel corso delle attività di programmazione e realizzazione del sistema hanno determinato una rimodulazione del progetto inizialmente delineato da questa Amministrazione.

In questo senso, è stato possibile accuratizzare il progetto, prevedendo la possibilità di:

- disporre di dati omogenei certificati relativi alla totalità dei voli intra-UE e extra-UE, in ingresso e in uscita dal territorio nazionale;
- acquisire un sofisticato software *ad hoc* dotato di numerose funzioni in grado di supportare in modo più efficace l'attività di analisi di dati PNR in relazione alla tipologia di reati che la Direttiva PNR mira a prevenire e contrastare.

In tale contesto, si evidenzia che nelle ipotesi iniziali era stato previsto di destinare una quota pari a euro 7.500.000 a gravare sui fondi stanziati dall'articolo 1, comma 608, della Legge 11 dicembre 2016, n. 232, per la realizzazione dei collegamenti tra il CEN di Napoli e il CED interforze – al fine di garantire l'ampliamento della connettività nonché la sicurezza del trasporto delle informazioni - necessari al più efficace funzionamento della piattaforma PNR. Considerato, tuttavia, che tali interventi costituiscono una realizzazione "a fattor comune" anche per altre funzionalità dell'Amministrazione della pubblica sicurezza, è emersa la necessità di ricorrere, indipendentemente dal progetto PNR, alle risorse previste dall'articolo 1, comma 140, della Legge 232/2016, a seguito di ripartizione dell'apposito fondo, avvenuta alla fine dell'anno 2017.

Conseguentemente, ciò ha "liberato" euro 7.500.000 previsti dall'articolo 1, comma 608, della Legge di bilancio 2016, che si programma di impiegare sempre per il progetto PNR, accrescendone le funzionalità e le potenzialità operative.

Ciò premesso, si riportano gli elementi che hanno portato alla quantificazione dei fabbisogni.

Per quanto riguarda i fondi ordinari di conto capitale stanziati dalla citata Legge n. 232 del 2016, pari a euro 21.500.000, in relazione alle annualità 2017 e 2018, sono stati attualmente impegnati circa euro 20.850.000 (comprensivi di IVA), secondo il seguente dettaglio:

- acquisto del servizio di ricezione di dati PNR e API qualificati e omogenei per un totale di euro 6.908.000;
- realizzazione del software per la gestione dei dati API: euro 9.600.000 per il software centralizzato, più euro 1.740.000 per il software degli Uffici di frontiera;
- acquisto del servizio di conduzione del sistema API/PNR per un totale di euro 2.600.000;

Per quanto concerne i fondi ISF, le somme saranno così ripartite:

- realizzazione software per la gestione dei dati PNR: euro 5.500.000;
- fornitura hardware e software a licenza per una spesa pari a euro 5.300.000, di cui:
  - realizzazione infrastruttura presso C.E.N. di Napoli ove sarà attestata la struttura centrale: euro 4.800.000;
  - esigenza di adeguamento dell'hardware per la sala server della Direzione Centrale della Polizia Criminale, presso la quale si attesterà l'UIP: euro 500.000;
- potenziamento dell'infrastruttura tecnologica necessario per garantire l'operatività dell'UIP nazionale (fornitura di hardware e software di base): euro 220.000.

Il quadro complessivo delle risorse, come sopra delineato, garantisce quindi che il recepimento della Direttiva PNR non richiede ulteriori interventi capaci di generare effetti di spesa: l'adeguamento dell'ordinamento interno sarà attuato con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Infatti, ad eccezione dei costi derivanti dalla realizzazione del Sistema Informativo, il decreto introduce norme di carattere procedurale e di natura ordinamentale o, comunque, norme la cui attuazione non richiede interventi tali da comportare nuovi o ulteriori dispendi di risorse pubbliche, come qui di seguito illustrato segnatamente per ogni disposizione.

Articoli 1, 2 e 3 (obiettivo, ambito di applicazione, definizioni e finalità dei trattamenti)

L'articolo 1 enuncia l'obiettivo dell'intervento normativo (attuazione della Direttiva PNR e assorbimento della normativa di attuazione della Direttiva API) e ne definisce l'ambito di applicazione.

L'articolo 2 detta norme di carattere definitorio, mentre l'articolo 3 enuncia le specifiche finalità per le quali deve essere effettuato il trattamento dei dati PNR e dei dati API.

Si tratta, quindi, di previsioni puramente ordinamentali, insuscettibili di determinare nuovi o ulteriori oneri a carico della finanza pubblica.

Articolo 4 (Sistema Informativo)

L'articolo 4 disciplina la realizzazione del Sistema Informativo dedicato alla trattazione dei dati PNR e dei dati API (comma 1). Per i profili di spesa riguardanti la creazione di tale *repository*, oltre a quanto già esplicitato in premessa, si specifica che tale attività prevede l'acquisto di un servizio per la realizzazione di un software *ad hoc* per la gestione dei dati API e PNR, nonché per la fornitura dell'hardware e del software a licenza.

Gli oneri per l'acquisto, pari a euro 9.600.000, sono imputati sul capitolo di bilancio 7505 di parte capitale, con riferimento al trattamento centralizzato dei dati API, e pari a euro 5.500.000, a valere sui fondi ISF, con riferimento al trattamento dei dati PNR.

Ulteriori oneri, pari a euro 2.600.000 a valere sul capitolo 7505, sono previsti per il servizio di conduzione operativa del Sistema informativo.

L'attuazione della disposizione comporta, infine, una spesa pari a euro 1.700.000 per l'acquisto dell'hardware, e una spesa pari a euro 3.820.000 per l'acquisto dei software a licenza, a valere sui fondi ISF.

Le disposizioni di cui ai commi 2, 3 e 4 regolano le condizioni di utilizzo del sistema e l'individuazione del titolare e dei responsabili del trattamento dei dati PNR e dei dati API. Si tratta di norme ordinamentali la cui attuazione non comporta nuovi o ulteriori oneri a carico del bilancio dello Stato.

Articolo 5 (implementazione del Sistema Informativo)

L'articolo 5 sancisce l'obbligo per i vettori aerei di trasferire i dati PNR al Sistema Informativo e ne prevede le specifiche modalità di adempimento.

La norme disciplina dunque oneri ad esclusivo carico dei predetti operatori economici ed è quindi insuscettibile di determinare conseguenze negative per la finanza pubblica.

Articolo 6 (Unità d'informazione sui passeggeri nazionale)

L'articolo 6 prevede che l'organizzazione dell'UIP nazionale sia definita con l'ordinario strumento del decreto del Ministro dell'Interno, adottato di concerto con il Ministro dell'Economia e della Finanze ai sensi dell'articolo 5, settimo comma, della Legge n. 121/1981 e la dotazione organica, anche della componente interforze, sia stabilita con il decreto del Presidente del Consiglio dei Ministri di cui all'articolo 6, secondo comma, della stessa Legge n. 121/1981. A riguardo si precisa che l'adozione di tali provvedimenti non implicherà nuovi o ulteriori aggravi a carico della finanza pubblica, in quanto ai nuovi fabbisogni di personale si provvederà con le risorse disponibili a legislazione vigente.

Sul punto, si precisa che la Direzione Centrale della Polizia Criminale dispone di una dotazione effettiva pari complessivamente a 1.052 unità (dato aggiornato al 16 novembre scorso), delle varie qualifiche e ruoli delle quattro Forze di polizia, oltreché dell'Amministrazione civile dell'Interno. Tale dotazione appare adeguata alle esigenze, alla luce del fatto che eventuali moderati bisogni di incremento del numero di personale possono essere soddisfatti attingendo ad altre articolazioni del Dipartimento della pubblica sicurezza, che conta oggi su un organico effettivo pari a circa 7.500 unità.

Il comma due reca norme di natura procedurale e come tali insuscettibili di determinare ulteriori oneri.

Articolo 7 (Uffici incaricati dei controlli di polizia di frontiera)

L'articolo 7 disciplina il trattamento dei dati API ad opera degli Uffici incaricati dei controlli di polizia di frontiera, configurando una delle tappe del processo di assorbimento, realizzato dal presente decreto, della normativa di attuazione della Direttiva API.

I dati API vengono attualmente trattati attraverso il Sistema informativo frontaliero *Border Control System* che, come anticipato in premessa, verrà sostituito dal Sistema Informativo di cui al presente decreto una volta entrato in funzione a pieno regime. Pertanto, i costi connessi alla messa a punto degli strumenti tecnici per il trattamento dei dati API effettuato dagli operatori di frontiera ammontano a euro 1.740.000, a valere sul capitolo 7505.

Il personale che effettuerà il trattamento dei dati API ai sensi del presente decreto è lo stesso che opera attualmente e, di conseguenza, l'attuazione di tale disposizione sarà assicurata con le risorse umane disponibili a legislazione vigente.

Articolo 8 e 9 (trattamento dei dati PNR e dei dati API)

Gli articoli 8 e 9 definiscono le modalità operative del trattamento dei dati PNR e dei dati API. Nell'ambito dei costi derivanti dalla realizzazione del Sistema Informativo utilizzato per la raccolta e il trattamento di entrambe le tipologie di dati, di cui si è parlato dettagliatamente in premessa e *sub* articolo 4, l'attività di trattamento dei dati PNR e API comporta l'acquisizione di un servizio che consenta di ricevere dati PNR e API qualificati e omogenei. Gli oneri per l'acquisto, pari a euro 6.908.000, sono imputati sul già citato capitolo di bilancio 7505 di parte capitale.

Gli articoli in esame, inoltre, dettano norme di carattere procedurale, dalla cui attuazione non derivano nuovi o ulteriori profili di spesa.

Articolo 10 (periodo di conservazione dei dati PNR e trasformazione in forma anonima)

L'articolo 10 regola le modalità di conservazione, di trasformazione in forma anonima e di cancellazione dei dati PNR e dei risultati del loro trattamento. Tali attività saranno garantite mediante il software *ad hoc* citato *sub* articolo 4, la cui copertura finanziaria sarà garantita mediante il ricorso ai fondi ISF.

Si disciplinano altresì le condizioni per il trasferimento delle informazioni alle autorità competenti e a Europol decorsi i sei mesi dalla trasmissione delle informazioni da parte dei vettori aerei, ossia una volta che è stata effettuata la procedura di mascheramento dei dati. Si

prevedono passaggi procedurali che costituiscono adempimenti di ridotta complessità e che pertanto non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Articolo 11 (conservazione dei dati API)

L'articolo 11, conformemente all'articolo 6 della Direttiva API, dispone l'obbligo per i vettori aerei di cancellare, entro ventiquattro ore dall'arrivo del volo, i dati API trasmessi. Si tratta dell'attribuzione di un onere, peraltro già vigente, a carico dei vettori aerei, insuscettibile di determinare aggravi per il bilancio dello Stato.

Articolo 12 (trasferimento dei dati PNR alle autorità competenti nazionali)

L'articolo 12 definisce le modalità con le quali l'UIP nazionale trasmette, d'iniziativa ovvero sulla base di una richiesta debitamente motivata, i dati PNR e i risultati del loro trattamento alle autorità competenti nazionali, prescrivendo l'utilizzo di strumenti informatici, secondo quanto previsto con i decreti di natura non regolamentare di cui all'articolo 4, comma 5, inerenti al funzionamento tecnico del Sistema Informativo e quindi dotati della copertura finanziaria indicata per l'articolo 4.

Per le trasmissioni dei dati in parola, così come per le trasmissioni previste dagli articoli da 13 a 18, sarà utilizzato il sistema SIENA, ovvero i consueti canali sicuri e protetti (PEC, MIC), nonché ogni altro canale di cooperazione internazionale di polizia, attraverso i quali già oggi si sviluppano le comunicazioni tra la Direzione Centrale della Polizia Criminale, presso la quale sarà istituita l'UIP nazionale, e le autorità. Atteso che i suddetti canali sostengono, ad oggi, un traffico in entrata e in uscita pari a circa 600.000 messaggi all'anno e che tali applicazioni sono in grado di supportare, senza inconvenienti, un incremento stimato del 15% nel triennio, si ritiene che tali strutture siano in grado di far fronte al flusso derivante dal trattamento dei dati PNR.

Le restanti previsioni della disposizione rivestono carattere eminentemente ordinamentale e procedurale e non comportano l'insorgenza di nuovi o ulteriori oneri per la finanza pubblica.

Articoli da 13 a 17 (scambio di dati PNR con le autorità competenti e con le UIP di altri Stati membri)

Gli articoli da 13 a 16 disciplinano le procedure e le condizioni in presenza delle quali l'UIP nazionale trasferisce o scambia i dati PNR e i risultati del loro trattamento con le autorità competenti e con le UIP di altri Stati membri. Si tratta di disposizioni aventi tenore procedurale, che presenterebbero profili di spesa solo nell'eventualità in cui si dovessero creare *ex novo* canali di comunicazione specificamente dedicati alla trasmissione reciproca dei dati PNR tra i citati attori istituzionali.

Tale eventualità è esclusa dalla previsione di cui all'articolo 17, che prescrive l'utilizzo dei canali di cooperazione internazionale di polizia già esistenti. Pertanto, la disposizione non comporta nuovi o maggiori oneri a carico della finanza pubblica.

Articolo 18 (trasferimento dei dati PNR a Europol)

L'articolo 18 detta le condizioni per il trasferimento dei dati PNR o dei risultati del loro trattamento a Europol.

Al verificarsi dei presupposti prescritti, l'UIP nazionale trasmette le informazioni a Europol utilizzando l'applicazione SIENA secondo le disposizioni di cui al regolamento (CE) 11 maggio 2016, n. 2016/794.

Anche in questo caso si prescrive l'utilizzo di un meccanismo di comunicazione già esistente e pertanto, in relazione ai profili di carattere finanziario, si richiamano le osservazioni formulate poco sopra per gli articoli dedicati al trasferimento e allo scambio delle informazioni con gli Stati membri e si escludono nuovi aggravi per il bilancio dello Stato.

Articolo 19 (trasferimento dei dati PNR ai Paesi terzi)

L'articolo 19 si occupa del trasferimento dei dati PNR e dei risultati del loro trattamento ai Paesi terzi, subordinandolo al verificarsi di stringenti presupposti e facendo salve le condizioni previste da eventuali accordi internazionali.

La norma contiene disposizioni di natura ordinamentale e non determina ricadute sui livelli della spesa pubblica, atteso che la trasmissione dei dati rientra nell'ordinaria attività di cooperazione giudiziaria e di polizia.

Articolo 20 (autorità nazionale di controllo)

L'articolo 20 individua l'"Autorità nazionale di controllo" (così come delineata dalla Direttiva PNR) nel Garante per la protezione dei dati personali e attribuisce espressamente allo stesso l'esercizio della funzione di controllo con le modalità previste dal Codice in materia di protezione dei dati personali.

Si tratta di una disposizione di carattere ordinamentale, che non attribuisce al Garante compiti ulteriori rispetto a quelli espletati nell'ambito delle ordinarie attività istituzionali e non comporta quindi nuovi o ulteriori oneri per la finanza pubblica.

Articolo 21 (responsabile per la protezione dei dati)

L'articolo 21 introduce la figura del responsabile della protezione dei dati e ne disciplina le attribuzioni e la posizione ordinamentale, collocandolo nell'ambito della Direzione Centrale della Polizia Criminale del Dipartimento della pubblica sicurezza del Ministero dell'Interno. La designazione dello specifico ufficio competente a svolgere le funzioni di responsabile della protezione dei dati si perfezionerà con un successivo decreto del Capo della Polizia – Direttore Generale della Pubblica Sicurezza, la cui attuazione sarà assicurata con le risorse umane e strumentali disponibili a legislazione vigente e, pertanto, a invarianza di spesa pubblica (si fa rinvio a quanto già illustrato relativamente all'articolo 6).

Articolo 22 (protezione dei dati personali)

L'articolo 22 stabilisce che in relazione ai trattamenti dei dati personali effettuati ai sensi del presente decreto trovano applicazione le misure già oggi contemplate dalle disposizioni del Codice per la protezione dei dati personali.

Si prescrivono anche specifici oneri per l'UIP nazionale volti a garantire la correttezza del trattamento dei dati e il rispetto delle norme previste in materia di protezione dei dati personali.

Si tratta di previsioni di carattere procedurale che non richiedono interventi tali da determinare ulteriori costi a carico del bilancio dello Stato, alla luce di quanto già riferito relativamente all'articolo 6.

Articolo 23 (diritti degli interessati)

L'articolo 23 riconosce ai soggetti interessati dai trattamenti di dati personali, effettuati nel contesto regolato dal presente decreto, i diritti che già oggi prevede l'articolo 10, commi 3, 4 e 5, della Legge 1 aprile 1981, n. 121, in relazione alle informazioni conservate nel Centro elaborazione dati. Sul punto, si precisa che le istanze presentate ai sensi del citato articolo 10, in relazione ai dati PNR, saranno trattate dal competente ufficio della Direzione Centrale della Polizia Criminale, il cui carico di lavoro ammonta attualmente a circa 6.100 istanze all'anno. Tale carico di lavoro è riferito a una mole di trattamenti effettuati dalle Forze di polizia significativamente cospicua. Rispetto a tale volume, l'incremento del numero di istanze, sebbene non quantificabile in termini esatti a priori, può considerarsi contenuto, sia in termini numerici, sia in termini di impegno richiesto. Ciò in quanto le questioni che potranno essere dibattute saranno riferite ad un numero naturalmente esiguo di soggetti "a rischio", e comunque richiederanno come verifica negli archivi di polizia dell'esistenza o meno di iscrizioni pregiudizievoli, ovvero di altre ricorrenze particolarmente significative.

Alla luce di ciò, l'incremento di attività amministrative derivante, su questo versante, dal provvedimento all'esame non determina nuovi o maggiori oneri a carico della finanza pubblica. Ciò anche alla luce di volumi organici della Direzione Centrale della Polizia Criminale e dell'intero Dipartimento della Pubblica Sicurezza descritti *sub* articolo 6.

Inoltre, viene riconosciuto all'interessato il diritto che sia data evidenza nel Sistema Informativo dell'esercizio dei propri diritti. Si tratta di una misura la cui implementazione non richiede interventi tali da determinare nuovi dispendi di risorse pubbliche.

Analoghe considerazioni valgono per le disposizioni ai sensi delle quali all'interessato devono essere comunicati i provvedimenti adottati a seguito dell'esercizio dei propri diritti e per le quali il Garante può disporre la rimozione dell'indicazione della citata evidenza nel Sistema Informativo.

Articolo 24 (sanzioni)

L'articolo 24 definisce le violazioni al presente decreto che rilevano ai fini sanzionatori, individuando le specifiche sanzioni amministrative e le autorità competenti a irrogarle.

Più in dettaglio, seppur con un aggravio nel trattamento sanzionatorio, viene sostanzialmente mutuato il meccanismo introdotto dalla normativa di attuazione della Direttiva API, già operante e, pertanto, insuscettibile di determinare l'insorgenza di nuovi o ulteriori aggravi per il bilancio dello Stato.

Articolo 25 (statistiche)

L'articolo 25 prevede l'onere per il Ministero dell'Interno di comunicare, annualmente, alla Commissione europea determinati dati statistici concernenti i dati PNR trasmessi all'UIP nazionale, senza determinare, in fase attuativa, nuovi dispendi di risorse pubbliche.

Articolo 26 (disposizioni transitorie e finali)

L'articolare 26 norma l'entrata in vigore del presente decreto e detta norme transitorie per il periodo necessario all'adozione dei provvedimenti attuativi.

La disposizione introduce altresì norme di coordinamento con la disciplina di attuazione della Direttiva API, resesi necessarie in considerazione dell'assorbimento della disciplina stessa disposto dall'articolo 1.

Articolo 27 (clausola di neutralità finanziaria)

Reca la clausola di neutralità finanziaria in coerenza con quanto stabilito dall'articolo 12, comma 2, della Legge di delegazione europea 2016-2017.

MODULARIO
INTERNO - 54

MOD. 4 UL

Ministero dell'Interno

UFFICIO AFFARI LEGISLATIVI E RELAZIONI PARLAMENTARI

Prot. n. 1721218/L2016-001947 Roma, data del protocollo

DICHIARAZIONE DI ESCLUSIONE DALL'AIR

ALLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI
- Al Capo del Dipartimento per gli Affari Giuridici e Legislativi

R O M A

Si richiede, ai sensi dell'art. 8, comma 1, lettera b) del D.P.C.M. 11 settembre 2008, n. 170, **l'esclusione dall'AIR** con riferimento allo schema di decreto legislativo recante: "Attuazione della direttiva 27 aprile 2016, n 2016/681/UE del Parlamento Europeo e del Consiglio sull'uso dei dati del codice di prenotazione (PNR) ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi", in quanto rientrante nella seguente categoria:

- atto normativo in materia di sicurezza interna ed esterna dello Stato.

Il Capo dell'Ufficio responsabile per le attività AIR e VIR
.....

Il Capo dell'Ufficio Legislativo
.....

VISTO
Roma, 6/12/2018

Il Capo del Dipartimenti per gli Affari Giuridici e Legislativi

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;

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 frontaliero 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.