

## III

(Atti adottati a norma del trattato UE)

## ATTI ADOTTATI A NORMA DEL TITOLO VI DEL TRATTATO UE

## DECISIONE 2007/533/GAI DEL CONSIGLIO

del 12 giugno 2007

## sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare l'articolo 30, paragrafo 1, lettere a) e b), l'articolo 31, paragrafo 1, lettere a) e b), e l'articolo 34, paragrafo 2, lettera c),

vista la proposta della Commissione,

visto il parere del Parlamento europeo <sup>(1)</sup>,

considerando quanto segue:

(1) Il sistema d'informazione Schengen («SIS»), istituito a norma delle disposizioni del titolo IV della convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni <sup>(2)</sup>, firmata il 19 giugno 1990 («convenzione di Schengen») e il suo sviluppo SIS 1+, rappresentano uno strumento fondamentale per l'applicazione delle disposizioni dell'acquis di Schengen integrate nell'ambito dell'Unione europea.

(2) L'incarico di sviluppare il SIS di seconda generazione («SIS II») è stato affidato alla Commissione con regolamento (CE) n. 2424/2001 del Consiglio <sup>(3)</sup> e decisione 2001/886/GAI del Consiglio, del 6 dicembre 2001, sullo sviluppo del sistema d'informazione Schengen di seconda generazione (SIS II) <sup>(4)</sup>. Il SIS II sostituirà il SIS creato a norma della convenzione di Schengen.

(3) La presente decisione costituisce la base giuridica necessaria per disciplinare il SIS II nelle materie rientranti nell'ambito di applicazione del trattato sull'Unione europea («trattato UE»). Il regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) <sup>(5)</sup>, costituisce la base giuridica necessaria per disciplinare il SIS II nelle materie rientranti nell'ambito di applicazione del trattato che istituisce la Comunità europea («trattato CE»).

(4) Il fatto che la base giuridica necessaria per disciplinare il SIS II consti di strumenti separati non pregiudica il principio secondo il quale il SIS II costituisce un unico sistema d'informazione che dovrebbe operare in quanto tale. È pertanto opportuno che alcune disposizioni di tali strumenti siano identiche.

(5) Il SIS II dovrebbe essere una misura compensativa che contribuisce a mantenere un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione europea, sostenendo la cooperazione operativa fra autorità di polizia e giudiziarie in campo penale.

<sup>(1)</sup> Parere del 25 ottobre 2006 (non ancora pubblicato nella Gazzetta ufficiale).

<sup>(2)</sup> GU L 239 del 22.9.2000, pag. 19. Convenzione modificata da ultimo dal regolamento (CE) n. 1160/2005 del Parlamento europeo e del Consiglio (GU L 191 del 22.7.2005, pag. 18).

<sup>(3)</sup> GU L 328 del 13.12.2001, pag. 4.

<sup>(4)</sup> GU L 328 del 13.12.2001, pag. 1.

<sup>(5)</sup> GU L 381 del 28.12.2006, pag. 4.

- (6) È necessario specificare gli obiettivi del SIS II, la sua architettura tecnica e il suo finanziamento, fissare regole sul suo esercizio e uso e definire le competenze, le categorie di dati da inserire nel sistema, le finalità dell'inserimento dei dati e i relativi criteri, le autorità abilitate ad accedere ai dati, l'interconnessione delle segnalazioni e ulteriori norme sul trattamento dei dati e sulla protezione dei dati personali.
- (7) Il SIS II dovrebbe includere un sistema centrale (SIS II centrale) e applicazioni nazionali. Le spese occasionate dall'esercizio del SIS II centrale e dalla relativa infrastruttura di comunicazione dovrebbero essere a carico del bilancio generale dell'Unione europea.
- (8) È necessario redigere un manuale recante le modalità dettagliate di scambio di talune informazioni supplementari relative all'azione richiesta con le segnalazioni. Le autorità nazionali di ciascuno Stato membro dovrebbero garantire lo scambio di tali informazioni.
- (9) Durante un periodo transitorio la Commissione dovrebbe essere responsabile della gestione operativa del SIS II centrale e di parti dell'infrastruttura di comunicazione. Tuttavia, per garantire un passaggio graduale al SIS II, essa può delegare, del tutto o in parte, queste competenze a due organismi nazionali del settore pubblico. A lungo termine e in seguito ad una valutazione d'impatto contenente un'analisi di merito sulle alternative dal punto di vista finanziario, operativo ed organizzativo e proposte legislative della Commissione, dovrebbe essere istituito un organo di gestione incaricato di svolgere tali compiti. Il periodo transitorio non dovrebbe protrarsi oltre cinque anni dalla data a decorrere dalla quale si applica la presente decisione.
- (10) Il SIS II dovrebbe contenere segnalazioni delle persone ricercate per l'arresto a fini di consegna e a fini di estradizione. Oltre alle segnalazioni, è opportuno prevedere lo scambio di informazioni supplementari necessarie ai fini delle procedure di consegna e estradizione. In particolare, è opportuno che nell'ambito del SIS II siano trattati i dati di cui all'articolo 8 della decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri <sup>(1)</sup>.
- (11) È opportuno contemplare la possibilità di aggiungere nel SIS II una traduzione dei dati complementari introdotti ai fini della consegna in forza del mandato d'arresto europeo o ai fini dell'extradizione.
- (12) Il SIS II dovrebbe contenere segnalazioni di persone scomparse per garantirne la tutela o prevenire minacce, di persone ricercate nell'ambito di un procedimento giudiziario, di persone e oggetti ai fini di un controllo discreto o di un controllo specifico e di oggetti a fini di sequestro o di prova in un procedimento penale.
- (13) Le segnalazioni non dovrebbero essere conservate nel SIS II oltre il periodo necessario per la realizzazione degli obiettivi per il quale sono state fornite. In linea generale, le segnalazioni di persone dovrebbero essere cancellate automaticamente dal SIS II dopo un periodo di tre anni. Le segnalazioni di oggetti inserite ai fini di un controllo discreto o di controllo specifico dovrebbero essere cancellate automaticamente dopo un periodo di cinque anni. Le segnalazioni di oggetti ai fini di sequestro o di prova in un procedimento penale dovrebbero essere cancellate automaticamente dopo un periodo di dieci anni. Le decisioni di conservare le segnalazioni di persone dovrebbero essere basate su una valutazione individuale approfondita. Gli Stati membri dovrebbero esaminare le segnalazioni di persone entro il periodo definito e tenere statistiche sul numero di segnalazioni di persone per le quali il periodo di conservazione è stato prolungato.
- (14) Il SIS II, per contribuire alla corretta identificazione degli interessati, dovrebbe consentire il trattamento di dati biometrici. Per la stessa ragione, il SIS II dovrebbe inoltre consentire il trattamento dei dati relativi a persone la cui identità è stata usurpata per evitare i disagi causati da errori di identificazione, fatte salve adeguate garanzie, fra cui il consenso dell'interessato e una rigorosa limitazione delle finalità per cui tali dati possono essere lecitamente elaborati.
- (15) Gli Stati membri dovrebbero avere la possibilità di aggiungere un indicatore di validità a una segnalazione, affinché non sia eseguita sul proprio territorio l'azione richiesta dalla segnalazione. Per le segnalazioni a scopo di arresto a fini di consegna è opportuno che la decisione non venga in alcun modo interpretata in modo da derogare o impedire l'applicazione delle disposizioni contenute nella decisione quadro 2002/584/GAI. La decisione di aggiungere un indicatore di validità a una segnalazione dovrebbe essere basata unicamente sui motivi di rifiuto previsti dalla suddetta decisione quadro.
- (16) Qualora un indicatore di validità sia stato aggiunto e il luogo di soggiorno della persona ricercata per l'arresto a fini di consegna sia stato individuato, il luogo di soggiorno dovrebbe essere sempre comunicato all'autorità giudiziaria emittente che deciderà eventualmente di trasmettere un mandato di arresto europeo all'autorità giudiziaria competente in conformità delle disposizioni della decisione quadro 2002/584/GAI.
- (17) Gli Stati membri dovrebbero avere la possibilità di stabilire connessioni fra le segnalazioni nel SIS II. La creazione di connessioni fra due o più segnalazioni da parte di uno Stato membro non dovrebbe incidere sull'azione da eseguire, né sui termini di conservazione o sui diritti di accesso alle segnalazioni.

<sup>(1)</sup> GU L 190 del 18.7.2002, pag. 1.

- (18) I dati trattati nel SIS II in applicazione della presente decisione non dovrebbero essere trasferiti a paesi terzi o a organizzazioni internazionali, né messi a loro disposizione. Tuttavia, è opportuno rafforzare la cooperazione tra l'Unione europea e l'Interpol promuovendo un efficace scambio di informazioni relative ai passaporti. In caso di trasferimento di dati personali dal SIS II all'Interpol, si dovrebbe prevedere un livello adeguato di protezione di tali dati, garantito da un accordo che offra garanzie e condizioni rigorose.
- (19) Tutti gli Stati membri hanno ratificato la convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale. La convenzione stabilisce le eccezioni e le restrizioni all'esercizio dei diritti e agli obblighi da quella previsti, entro certi limiti. È opportuno che i dati personali elaborati ai fini dell'attuazione della presente decisione siano protetti secondo i principi enunciati nella convenzione. Laddove necessario, la presente decisione dovrebbe integrare o precisare i principi della convenzione.
- (20) Quando le autorità di polizia elaborano dati personali in applicazione della presente decisione occorrerebbe tener conto dei principi contenuti nella raccomandazione R (87) 15, del 17 settembre 1987, del comitato dei ministri del Consiglio d'Europa tendente a regolare l'uso dei dati di natura personale nel settore della polizia.
- (21) La Commissione ha presentato al Consiglio una proposta di decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, che dovrebbe essere approvata entro il 2006 e applicata ai dati personali trattati nell'ambito del sistema d'informazione Schengen di seconda generazione nonché al relativo scambio delle informazioni supplementari a norma della presente decisione.
- (22) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati <sup>(1)</sup>, in particolare le disposizioni dello stesso per quanto riguarda la riservatezza e la sicurezza del trattamento, si applicano al trattamento di dati personali da parte delle istituzioni e degli organismi comunitari nell'esercizio dei loro compiti di gestione operativa del SIS II nell'ambito dell'esercizio di attività che rientrano in tutto o in parte nell'ambito di applicazione del diritto comunitario. Parte del trattamento dei dati personali nell'ambito del SIS II rientra nell'ambito d'applicazione del diritto comunitario. Per un'applicazione coerente e omogenea delle norme relative alla tutela delle libertà e dei diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali occorre precisare che, quando la Commissione elabora dati personali a norma della presente decisione, si applica il regolamento (CE) n. 45/2001. Laddove necessario, è opportuno che i principi enunciati nel regolamento (CE) n. 45/2001 siano integrati o precisati dalla presente decisione.
- (23) Per quanto riguarda la riservatezza, le pertinenti disposizioni dello statuto dei funzionari delle Comunità europee e del regime applicabile agli altri agenti di dette Comunità dovrebbero applicarsi ai funzionari o altri agenti che sono impiegati e che lavorano per il SIS II.
- (24) È opportuno che le autorità nazionali di controllo controllino la liceità del trattamento dei dati personali effettuato dagli Stati membri, mentre il garante europeo della protezione dei dati istituito con decisione 2004/55/CE del Parlamento europeo e del Consiglio, del 22 dicembre 2003, relativa alla nomina dell'autorità di controllo indipendente prevista dall'articolo 286 del trattato CE <sup>(2)</sup>, dovrebbe controllare le attività delle istituzioni e degli organismi comunitari attinenti al trattamento dei dati personali tenuto conto dei compiti limitati svolti dalle istituzioni e dagli organismi comunitari riguardo ai dati stessi.
- (25) Gli Stati membri e la Commissione dovrebbero redigere un piano di sicurezza per agevolare l'attuazione degli obblighi in materia di sicurezza e dovrebbero cooperare tra loro al fine di affrontare le questioni di sicurezza da una prospettiva comune.
- (26) Al trattamento dei dati SIS II da parte di Europol si applicano le disposizioni in materia di protezione dei dati della convenzione del 26 luglio 1995 che istituisce un ufficio europeo di polizia <sup>(3)</sup> (di seguito «convenzione Europol»), in particolare quelle relative al potere dell'autorità di controllo comune, istituita dalla convenzione Europol, di sorvegliare le attività di Europol, e le disposizioni relative alla responsabilità in caso di trattamento illecito dei dati personali da parte di quest'ultimo.
- (27) Al trattamento dei dati SIS II da parte di Eurojust si applicano le disposizioni in materia di protezione dei dati della decisione 2002/187/GAI, del 28 febbraio 2002, che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità <sup>(4)</sup>, in particolare quelle relative al potere dell'autorità di controllo comune, istituita da detta decisione, di sorvegliare le attività di Eurojust, e le disposizioni relative alla responsabilità in caso di trattamento illecito dei dati personali da parte di quest'ultima.

<sup>(2)</sup> GU L 12 del 17.1.2004, pag. 47.

<sup>(3)</sup> GU C 316 del 27.11.1995, pag. 2.

<sup>(4)</sup> GU L 63 del 6.3.2002, pag. 1.

<sup>(1)</sup> GU L 8 del 12.1.2001, pag. 1.

- (28) Per ragioni di trasparenza è opportuno che ogni due anni la Commissione o, se previsto, l'organo di gestione presenti una relazione sul funzionamento tecnico del SIS II centrale e dell'infrastruttura di comunicazione, compresa la sua sicurezza, e sullo scambio di informazioni supplementari. Ogni quattro anni la Commissione dovrebbe provvedere a una valutazione globale.
- (29) A causa della loro tecnicità, del loro livello di dettaglio e della necessità di aggiornamenti periodici la presente decisione non può trattare con eshaustività taluni aspetti del SIS II quali le norme tecniche concernenti l'inserimento di dati, inclusi i dati necessari per l'inserimento di una segnalazione, l'aggiornamento, la cancellazione e la consultazione dei dati, le norme sulla compatibilità e la priorità delle segnalazioni, l'aggiunta di indicatori di validità, l'interconnessione delle segnalazioni e lo scambio di informazioni supplementari. È pertanto opportuno delegare alla Commissione competenze di esecuzione in relazione ai citati aspetti. Le norme tecniche concernenti la consultazione delle segnalazioni dovrebbero tener conto del corretto funzionamento delle applicazioni nazionali. Previa una valutazione d'impatto effettuata dalla Commissione, si dovrebbe decidere in quale misura le disposizioni di attuazione potrebbero essere di competenza dell'organo di gestione, una volta istituito.
- (30) La presente decisione dovrebbe definire la procedura per l'adozione delle misure necessarie alla sua attuazione. È opportuno che la procedura per l'adozione delle disposizioni di attuazione a norma della presente decisione e del regolamento (CE) n. 1987/2006 sia la stessa.
- (31) È opportuno stabilire disposizioni transitorie relative alle segnalazioni effettuate nel SIS 1+ che devono essere trasferite nel SIS II. È opportuno che per un periodo limitato, fino a quando cioè gli Stati membri non abbiano esaminato la compatibilità di queste segnalazioni con il nuovo quadro giuridico, continuino a applicarsi alcune disposizioni dell'acquis di Schengen. La compatibilità delle segnalazioni di persone dovrebbe essere esaminata in via prioritaria. Inoltre, qualsiasi modifica, complemento, rettifica o aggiornamento di una segnalazione trasferita dal SIS 1+ al SIS II, nonché qualsiasi risposta positiva su tale segnalazione, dovrebbe attivare l'esame immediato della sua compatibilità con le disposizioni della presente decisione.
- (32) È necessario stabilire disposizioni specifiche riguardo alla parte del bilancio assegnata alle operazioni del SIS che non rientrano nel bilancio generale dell'Unione europea.
- (33) Poiché gli obiettivi dell'azione prevista, vale a dire l'istituzione e la regolamentazione di un sistema comune d'informazione, non possono essere realizzati in misura sufficiente dagli Stati membri e possono dunque, a causa delle dimensioni o degli effetti dell'azione in questione, essere realizzati meglio a livello dell'Unione europea, il Consiglio può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato CE e richiamato nell'articolo 2 del trattato UE. In ottemperanza al principio di proporzionalità enunciato nello stesso articolo 5 del trattato CE, la presente decisione si limita a quanto è necessario per conseguire tali obiettivi.
- (34) La presente decisione rispetta i diritti fondamentali e osserva i principi riconosciuti in particolare dalla carta dei diritti fondamentali dell'Unione europea.
- (35) Il Regno Unito partecipa alla presente decisione a norma dell'articolo 5 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea allegato al trattato UE e al trattato CE, e dell'articolo 8, paragrafo 2, della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune delle disposizioni dell'acquis di Schengen <sup>(1)</sup>.
- (36) L'Irlanda partecipa alla presente decisione a norma dell'articolo 5 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea allegato al trattato UE e al trattato CE, e dell'articolo 6, paragrafo 2, della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen <sup>(2)</sup>.
- (37) La presente decisione non pregiudica le disposizioni concernenti la partecipazione parziale del Regno Unito e dell'Irlanda all'acquis di Schengen definite, rispettivamente, nella decisione 2000/365/CE e nella decisione 2002/192/CE.
- (38) Per quanto riguarda l'Islanda e la Norvegia, la presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen <sup>(3)</sup>, che rientrano nel settore di cui all'articolo 1, punto G, della decisione 1999/437/CE del Consiglio <sup>(4)</sup>, relativa a talune modalità di applicazione dell'accordo.
- (39) È opportuno definire un regime per permettere a rappresentanti dell'Islanda e della Norvegia di essere associati ai lavori dei comitati che assistono la Commissione nell'esercizio delle sue competenze d'esecuzione. Tale regime è stato previsto nello scambio di lettere tra il Consiglio dell'Unione europea e la Repubblica d'Islanda e il Regno di Norvegia sui comitati che coadiuvano la Commissione europea nell'esercizio dei suoi poteri esecutivi <sup>(5)</sup>, allegato al summenzionato accordo.

(1) GU L 131 dell'1.6.2000, pag. 43.

(2) GU L 64 del 7.3.2002, pag. 20.

(3) GU L 176 del 10.7.1999, pag. 36.

(4) GU L 176 del 10.7.1999, pag. 31.

(5) GU L 176 del 10.7.1999, pag. 53.

(40) Per quanto riguarda la Svizzera, la presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo firmato dall'Unione europea, dalla Comunità europea e dalla Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen, che rientrano nel settore di cui all'articolo 1, punto G, della decisione 1999/437/CE, in combinato disposto con l'articolo 4, paragrafo 1, delle decisioni del Consiglio 2004/849/CE <sup>(1)</sup> e 2004/860/CE <sup>(2)</sup>.

(41) È opportuno definire un regime per consentire a rappresentanti della Svizzera di essere associati ai lavori dei comitati che assistono la Commissione nell'esercizio delle sue competenze d'esecuzione. Tale regime è stato previsto nello scambio di lettere tra la Comunità e la Svizzera, allegato al summenzionato accordo.

(42) La presente decisione costituisce un atto basato sull'acquis di Schengen o ad esso altrimenti connesso ai sensi dell'articolo 3, paragrafo 2, dell'atto di adesione del 2003 e dell'articolo 4, paragrafo 2, dell'atto di adesione del 2005.

(43) La presente decisione dovrebbe applicarsi al Regno Unito, all'Irlanda e alla Svizzera alle date stabilite secondo le procedure definite nei pertinenti strumenti relativi all'applicazione dell'acquis di Schengen a tali Stati,

DECIDE:

#### CAPO I

### DISPOSIZIONI GENERALI

#### Articolo 1

### Istituzione e scopo generale del SIS II

1. È istituito il sistema d'informazione Schengen di seconda generazione («SIS II»).

2. Scopo del SIS II è, a norma della presente decisione, assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione europea, incluso il mantenimento

<sup>(1)</sup> Decisione 2004/849/CE del Consiglio, del 25 ottobre 2004, relativa alla firma, a nome dell'Unione europea, nonché all'applicazione provvisoria di alcune disposizioni dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen (GU L 368 del 15.12.2004, pag. 26).

<sup>(2)</sup> Decisione 2004/860/CE del Consiglio, del 25 ottobre 2004, relativa alla firma, a nome della Comunità europea, nonché all'applicazione provvisoria di alcune disposizioni dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen (GU L 370 del 17.12.2004, pag. 78).

della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri e applicare le disposizioni della parte terza, titolo IV, del trattato CE relativo alla circolazione delle persone in detto territorio avvalendosi delle informazioni trasmesse tramite tale sistema.

#### Articolo 2

### Ambito di applicazione

1. La presente decisione definisce le condizioni e le procedure applicabili all'inserimento e al trattamento nel SIS II delle segnalazioni relative a persone e oggetti, allo scambio di informazioni supplementari e dati complementari per la cooperazione di polizia e giudiziaria in campo penale.

2. La presente decisione contempla anche disposizioni sull'architettura tecnica del SIS II, sulle competenze degli Stati membri e dell'organo di gestione di cui all'articolo 15, sulle regole generali sul trattamento dei dati, sui diritti delle persone e sulla responsabilità.

#### Articolo 3

### Definizioni

1. Ai fini della presente decisione, si intende per:

- a) «segnalazione»: un insieme di dati inseriti nel SIS II che permetta alle autorità competenti di identificare un individuo o un oggetto in vista di intraprendere un'azione specifica;
- b) «informazioni supplementari»: le informazioni non memorizzate nel SIS II ma connesse alle segnalazioni del SIS II, che devono essere scambiate:
  - i) per permettere agli Stati membri di consultarsi o informarsi a vicenda quando introducono una segnalazione;
  - ii) in seguito a una risposta positiva al fine di consentire l'azione appropriata;
  - iii) quando non è possibile procedere all'azione richiesta;
  - iv) con riguardo alla qualità dei dati SIS II;
  - v) con riguardo alla compatibilità e alla priorità delle segnalazioni;
  - vi) con riguardo ai diritti di accesso;
- c) «dati complementari»: i dati memorizzati nel SIS II e connessi alle segnalazioni del SIS II, che devono essere immediatamente disponibili per le autorità competenti nei casi in cui una persona i cui dati sono stati inseriti nel SIS II sia individuata grazie all'interrogazione di tale sistema;

- d) «dati personali»: qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); una persona identificabile è una persona che può essere identificata, direttamente o indirettamente;
- e) «trattamento di dati personali» («trattamento»): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come raccolta, registrazione, organizzazione, memorizzazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, nonché blocco, cancellazione o distruzione.

2. Nella presente decisione qualsiasi riferimento alle disposizioni della decisione quadro 2002/584/GAI si intende fatto altresì alle corrispondenti disposizioni degli accordi conclusi tra l'Unione europea e i paesi terzi in virtù degli articoli 24 e 38 del trattato UE ai fini della consegna di persone sulla base di un mandato di arresto, che prevedono che il mandato di arresto sia trasmesso tramite il sistema di informazione Schengen.

#### Articolo 4

##### Architettura tecnica e modalità operative del SIS II

1. Il SIS II consta di:
- a) un sistema centrale («SIS II centrale») costituito da:
- un'unità di supporto tecnico («CS-SIS») contenente una banca dati, la «banca dati del SIS II»,
  - un'interfaccia nazionale uniforme («NI-SIS»);
- b) un sistema nazionale («N.SIS II») in ciascuno Stato membro, consistente nei sistemi di dati nazionali che comunicano con il SIS II centrale. Un N.SIS II può contenere un archivio di dati («copia nazionale»), costituito da una copia completa o parziale della banca dati del SIS II;
- c) un'infrastruttura di comunicazione fra il CS-SIS e l'NI-SIS (l'«infrastruttura di comunicazione») che è dotata di una rete virtuale cifrata dedicata ai dati SIS II e provvede allo scambio di informazioni tra uffici Sirene ai sensi dell'articolo 7, paragrafo 2.

2. I dati SIS II sono inseriti, aggiornati, cancellati e consultati attraverso i vari sistemi N.SIS II. La copia nazionale è disponibile ai fini dell'interrogazione automatizzata nel territorio di ciascuno degli Stati membri che usano tale copia. Non possono essere consultati gli archivi di dati contenuti nell'N.SIS II degli altri Stati membri.

3. Il CS-SIS svolge funzioni di controllo e gestione tecnici, ha sede a Strasburgo (Francia), mentre il CS SIS di riserva, in grado di assicurare tutte le funzioni del CS SIS principale in caso di guasto di tale sistema, ha sede a Sankt Johann im Pongau (Austria).

4. Il CS-SIS fornisce i servizi necessari per l'inserimento e il trattamento dei dati SIS II, compresa la consultazione della banca dati del SIS II. Agli Stati membri che usano una copia nazionale, il CS-SIS:

- a) fornisce l'aggiornamento in linea delle copie nazionali;
- b) assicura la sincronizzazione e la coerenza tra le copie nazionali e la banca dati del SIS II;
- c) fornisce le funzioni di inizializzazione e ripristino delle copie nazionali.

#### Articolo 5

##### Costi

1. I costi relativi all'istituzione, all'esercizio e alla manutenzione del SIS II centrale e dell'infrastruttura di comunicazione sono a carico del bilancio generale dell'Unione europea.

2. Tali costi includono il lavoro effettuato con riguardo al CS-SIS per garantire la fornitura dei servizi di cui all'articolo 4, paragrafo 4.

3. I costi per l'istituzione, l'esercizio e la manutenzione di ciascun N.SIS II sono a carico dello Stato membro interessato.

#### CAPO II

##### COMPETENZE DEGLI STATI MEMBRI

#### Articolo 6

##### Sistemi nazionali

Ciascuno Stato membro è competente per l'istituzione, l'esercizio e la manutenzione del suo N.SIS II e per il collegamento del suo N.SIS II all'NI-SIS.

#### Articolo 7

##### Ufficio N.SIS II e ufficio Sirene

1. Ciascuno Stato membro designa un'autorità («ufficio N.SIS II») che ha la competenza centrale per il rispettivo N.SIS II.

Tale autorità è responsabile del corretto funzionamento e della sicurezza dell'N.SIS II, garantisce l'accesso delle autorità competenti al SIS II e adotta le misure atte a garantire l'osservanza delle disposizioni della presente decisione.

Ciascuno Stato membro trasmette le proprie segnalazioni per il tramite del proprio ufficio N.SIS II.

2. Ciascuno Stato membro designa l'autorità competente per lo scambio di tutte le informazioni supplementari («ufficio Sirene») conformemente alle disposizioni del manuale Sirene di cui all'articolo 8.

Detti uffici coordinano inoltre la verifica della qualità delle informazioni inserite nel SIS II. A tali fini, essi hanno accesso ai dati elaborati nel SIS II.

3. Gli Stati membri comunicano all'organo di gestione il rispettivo ufficio N.SIS II e ufficio Sirene. L'organo di gestione ne pubblica l'elenco insieme all'elenco di cui all'articolo 46, paragrafo 8.

#### Articolo 8

##### **Scambio di informazioni supplementari**

1. Le informazioni supplementari sono scambiate conformemente alle disposizioni del manuale Sirene e per il tramite dell'infrastruttura di comunicazione. In caso di indisponibilità dell'infrastruttura di comunicazione, gli Stati membri possono usare altri mezzi tecnici adeguatamente protetti per lo scambio di informazioni supplementari.

2. Le informazioni supplementari sono usate solo per lo scopo per il quale sono state trasmesse.

3. Alle richieste di informazioni supplementari formulate dagli altri Stati membri è data una risposta quanto più rapida possibile.

4. Le modalità dettagliate di scambio delle informazioni supplementari sono adottate secondo la procedura di cui all'articolo 67 sotto forma di un manuale denominato «manuale Sirene», fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.

#### Articolo 9

##### **Compatibilità tecnica**

1. Per consentire una pronta ed efficiente trasmissione dei dati, all'atto dell'istituzione del rispettivo N.SIS II ciascuno Stato membro si conforma ai protocolli e alle procedure tecniche stabiliti per assicurare la compatibilità del proprio N.SIS II con il CS-SIS. Tali protocolli e procedure tecniche sono stabiliti secondo la procedura di cui all'articolo 67, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.

2. In caso di uso di una copia nazionale, lo Stato membro interessato provvede, tramite i servizi forniti dal CS SIS, affinché i dati memorizzati nella copia nazionale siano, grazie agli aggiornamenti automatici di cui all'articolo 4, paragrafo 4, identici e coerenti con quelli della banca dati del SIS II e un'interrogazione nella sua copia nazionale produca risultati equivalenti a quelli di un'interrogazione effettuata nella banca dati del SIS II.

#### Articolo 10

##### **Sicurezza — Stati membri**

1. Ciascuno Stato membro adotta, per il rispettivo N.SIS II, le misure necessarie, compreso un piano di sicurezza, per:

- a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani di emergenza per la protezione delle infrastrutture critiche;
- b) impedire alle persone non autorizzate l'accesso alle installazioni informatiche utilizzate per il trattamento di dati personali (controlli all'ingresso delle installazioni);
- c) impedire che supporti di dati possano essere letti, copiati, modificati o asportati senza autorizzazione (controllo dei supporti di dati);
- d) impedire che i dati siano inseriti senza autorizzazione e che i dati personali memorizzati siano visionati, modificati o cancellati senza autorizzazione (controllo dell'archiviazione);
- e) impedire che persone non autorizzate usino i sistemi automatizzati di elaborazione dati mediante apparecchiature per la trasmissione di dati (controllo degli utenti);
- f) garantire che le persone autorizzate a usare un sistema automatizzato di elaborazione dati possano accedere solo ai dati di loro competenza attraverso identità di utente individuali e uniche ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);
- g) assicurare che tutte le autorità con diritto di accedere al SIS II o alle installazioni di elaborazione dati creino profili che descrivono i compiti e le funzioni delle persone autorizzate ad accedere, inserire, aggiornare, cancellare e consultare i dati e mettano senza indugio tali profili a disposizione delle autorità nazionali di controllo di cui all'articolo 60 a richiesta di queste (profili personali);
- h) garantire la possibilità di verificare ed accertare a quali organismi possano essere trasmessi dati personali mediante apparecchiature per la trasmissione di dati (controllo della trasmissione);
- i) garantire la possibilità di verificare ed accertare a posteriori quali dati personali siano stati introdotti nei sistemi automatizzati di elaborazione dati, il momento dell'inserimento, la persona che lo ha effettuato e lo scopo dello stesso (controllo dell'inserimento);
- j) impedire, in particolare mediante tecniche appropriate di cifratura, che all'atto del trasferimento di dati personali nonché del trasporto di supporti di dati essi possano essere letti, copiati, modificati o cancellati senza autorizzazione (controllo del trasporto);
- k) controllare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure di carattere organizzativo relative al controllo interno per garantire l'osservanza della presente decisione (autocontrollo).

2. Gli Stati membri adottano misure equivalenti a quelle del paragrafo 1 per quanto riguarda la sicurezza degli scambi di informazioni supplementari.

#### Articolo 11

### Riservatezza — Stati membri

Ogni Stato membro applica le proprie norme nazionali in materia di segreto professionale o altri obblighi di riservatezza equivalenti a tutti i soggetti e organismi che debbano lavorare con i dati SIS II e con le informazioni supplementari, conformemente alla propria legislazione nazionale. Tale obbligo vincola tali soggetti e organismi anche dopo che avranno rispettivamente lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

#### Articolo 12

### Tenuta dei registri a livello nazionale

1. Gli Stati membri che non usano copie nazionali provvedono affinché ogni accesso ai dati personali e ogni scambio dei medesimi nell'ambito del CS-SIS sia registrato nel proprio N.SIS II per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati, ai fini dell'autocontrollo e per garantire il corretto funzionamento di N.SIS II, l'integrità e la sicurezza dei dati.

2. Gli Stati membri che usano copie nazionali provvedono affinché ogni accesso ai dati SIS II e tutti gli scambi dei medesimi siano registrati ai fini di cui al paragrafo 1. Ciò non vale per i trattamenti di cui all'articolo 4, paragrafo 4.

3. I registri riportano, in particolare, la cronistoria delle segnalazioni, la data e l'ora della trasmissione dei dati, i dati usati per effettuare un'interrogazione, un riferimento ai dati trasmessi e il nome dell'autorità competente e del responsabile del trattamento dei dati.

4. I registri possono essere usati solo ai fini specificati di cui ai paragrafi 1 e 2 e sono cancellati al più presto un anno dopo e al più tardi tre anni dopo la loro creazione. I registri contenenti la cronistoria delle segnalazioni sono cancellati da uno a tre anni dopo la cancellazione delle segnalazioni.

5. I registri possono essere tenuti più a lungo se sono necessari per procedure di controllo già in corso.

6. Le autorità nazionali competenti incaricate di verificare la legittimità dell'interrogazione, di controllare la liceità del trattamento dei dati, dell'autocontrollo e di garantire il corretto funzionamento dell'N.SIS II, l'integrità e la sicurezza dei dati hanno accesso a tali registri, nei limiti delle rispettive competenze e su loro richiesta, ai fini dell'assolvimento dei loro doveri.

#### Articolo 13

### Autocontrollo

Gli Stati membri provvedono affinché ogni autorità con diritto di accesso ai dati SIS II adotti le misure necessarie per assicurare l'osservanza della presente decisione e cooperi, se necessario, con l'autorità nazionale di controllo.

#### Articolo 14

### Formazione del personale

Prima di essere autorizzato a elaborare dati memorizzati nel SIS II, il personale delle autorità con diritto di accesso al SIS II riceve una formazione adeguata sulle norme in materia di sicurezza e di protezione dei dati ed è informato dei reati e delle sanzioni pertinenti.

#### CAPO III

### COMPETENZE DELL'ORGANO DI GESTIONE

#### Articolo 15

### Gestione operativa

1. Dopo un periodo transitorio un organo di gestione (l'«organo di gestione»), finanziato dal bilancio generale dell'Unione europea, è responsabile della gestione operativa del SIS II centrale. L'organo di gestione, in collaborazione con gli Stati membri, provvede affinché in ogni momento le migliori tecnologie disponibili, fatta salva un'analisi costi-benefici, siano utilizzate per il SIS II centrale.

2. L'organo di gestione è responsabile altresì dei seguenti compiti connessi con l'infrastruttura di comunicazione:

- a) controllo;
- b) sicurezza;
- c) coordinamento dei rapporti tra gli Stati membri e il gestore.

3. La Commissione è responsabile di tutti gli altri compiti connessi con l'infrastruttura di comunicazione, in particolare:

- a) compiti relativi all'esecuzione del bilancio;
- b) acquisizione e rinnovo;
- c) aspetti contrattuali.



4. Durante un periodo transitorio, prima che l'organo di gestione assuma le sue responsabilità, la Commissione è responsabile della gestione operativa del SIS II centrale. La Commissione può delegare tale compito e compiti relativi all'esecuzione del bilancio a organismi nazionali del settore pubblico di due diversi paesi, a norma del regolamento (CE, Euratom) n. 1605/2002 del Consiglio, del 25 giugno 2002, che stabilisce il regolamento finanziario applicabile al bilancio generale delle Comunità europee <sup>(1)</sup>.

5. Ogni organismo nazionale del settore pubblico di cui al paragrafo 4 soddisfa, in particolare, i seguenti criteri di selezione:

- a) deve dimostrare che ha maturato una lunga esperienza nell'esercizio di un sistema d'informazione su larga scala dotato delle funzioni di cui all'articolo 4, paragrafo 4;
- b) deve possedere conoscenze specialistiche notevoli in materia di requisiti di funzionamento e di sicurezza di un sistema d'informazione dotato di funzioni paragonabili a quelle di cui all'articolo 4, paragrafo 4;
- c) deve disporre di un personale sufficiente ed esperto, con competenze professionali e conoscenze linguistiche adeguate per lavorare in un ambiente di cooperazione internazionale come quello richiesto dal SIS II;
- d) deve disporre di un'infrastruttura sicura costituita da installazioni e appositamente costruita, capace, in particolare, di sostenere e garantire il funzionamento continuo di sistemi IT su larga scala; e
- e) il suo contesto amministrativo deve permettergli di adempiere adeguatamente ai propri compiti ed evitare conflitti d'interesse.

6. Prima di ogni delega di cui al paragrafo 4 e poi a intervalli regolari, la Commissione informa il Parlamento europeo e il Consiglio in merito alle condizioni della delega, alla sua portata precisa e agli organismi ai quali i compiti sono delegati.

7. Qualora durante il periodo transitorio la Commissione deleghi la propria responsabilità a norma del paragrafo 4, provvede ad assicurare che tale delega rispetti pienamente i limiti posti dal sistema istituzionale stabilito nel trattato CE. Essa assicura in particolare che la delega non si ripercuota negativamente sull'efficacia dei meccanismi di controllo previsti dal diritto dell'Unione europea, siano essi a cura della Corte di giustizia, della Corte dei conti o del garante europeo della protezione dei dati.

8. La gestione operativa del SIS II centrale consiste nell'insieme dei compiti necessari al funzionamento 24 ore su 24 e 7 giorni su 7 del SIS II centrale, ai sensi della presente decisione, e comprende in particolare le attività di manutenzione e gli adattamenti tecnici necessari per un buon funzionamento del sistema.

## Articolo 16

### Sicurezza

1. L'organo di gestione e la Commissione adottano, rispettivamente per il SIS II centrale e per l'infrastruttura di comunicazione le misure necessarie, compreso un piano di sicurezza, per:

- a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani di emergenza per la protezione delle infrastrutture critiche;
- b) impedire alle persone non autorizzate l'accesso alle installazioni informatiche utilizzate per il trattamento di dati personali (controlli all'ingresso delle installazioni);
- c) impedire che supporti di dati possano essere letti, copiati, modificati o asportati senza autorizzazione (controllo dei supporti di dati);
- d) impedire che i dati siano inseriti senza autorizzazione e che i dati personali memorizzati siano visionati, modificati o cancellati senza autorizzazione (controllo dell'archiviazione);
- e) impedire che persone non autorizzate usino i sistemi automatizzati di elaborazione dati mediante apparecchiature per la trasmissione di dati (controllo degli utenti);
- f) garantire che le persone autorizzate a usare un sistema automatizzato di elaborazione dati possano accedere solo ai dati di loro competenza attraverso identità di utente individuali e uniche ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);
- g) creare profili che descrivano i compiti e le funzioni delle persone autorizzate ad accedere ai dati o alle installazioni informatiche e mettere senza indugio tali profili a disposizione del garante europeo della protezione dei dati di cui all'articolo 61 a richiesta di quest'ultimo (profili personali);
- h) garantire la possibilità di verificare ed accertare a quali organismi possano essere trasmessi dati personali mediante apparecchiature per la trasmissione di dati (controllo della trasmissione);
- i) garantire la possibilità di verificare ed accertare a posteriori quali dati personali siano stati introdotti nei sistemi automatizzati di elaborazione dati, il momento dell'inserimento e la persona che lo ha effettuato (controllo dell'inserimento);
- j) impedire, in particolare mediante tecniche appropriate di cifratura, che all'atto del trasferimento di dati personali nonché del trasporto di supporti di dati essi possano essere letti, copiati, modificati o cancellati senza autorizzazione (controllo del trasporto);
- k) controllare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure di carattere organizzativo relative al controllo interno per garantire l'osservanza della presente decisione (autocontrollo).

<sup>(1)</sup> GU L 248 del 16.9.2002, pag. 1.

2. L'organo di gestione adotta misure equivalenti a quelle di cui al paragrafo 1 per quanto riguarda la sicurezza degli scambi di informazioni supplementari attraverso l'infrastruttura di comunicazione.

#### Articolo 17

##### **Riservatezza — Organo di gestione**

1. Fatto salvo l'articolo 17 dello statuto dei funzionari delle Comunità europee, l'organo di gestione applica norme adeguate in materia di segreto professionale o altri obblighi di riservatezza equivalenti a tutti i membri del proprio personale che debbano lavorare con i dati SIS II, secondo standard equiparabili a quelli previsti all'articolo 11 della presente decisione. Tale obbligo vincola gli interessati anche dopo che avranno rispettivamente lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

2. L'organo di gestione adotta misure equivalenti a quelle di cui al paragrafo 1 per quanto riguarda la riservatezza degli scambi di informazioni supplementari attraverso l'infrastruttura di comunicazione.

#### Articolo 18

##### **Tenuta dei registri a livello centrale**

1. L'organo di gestione provvede affinché ogni accesso e ogni scambio di dati personali nell'ambito del CS-SIS siano registrati ai fini di cui all'articolo 12, paragrafi 1 e 2.

2. I registri riportano, in particolare, la cronistoria delle segnalazioni, la data e l'ora della trasmissione dei dati, i dati usati per effettuare interrogazioni, il riferimento ai dati trasmessi e l'identità dell'autorità competente responsabile del trattamento dei dati.

3. I registri possono essere usati solo ai fini di cui al paragrafo 1 e sono cancellati al più presto un anno dopo e al più tardi tre anni dopo la loro creazione. I registri contenenti la cronistoria delle segnalazioni sono cancellati da uno a tre anni dopo la cancellazione delle segnalazioni.

4. I registri possono essere tenuti più a lungo se sono necessari per procedure di controllo in corso.

5. Le autorità competenti incaricate di verificare la legittimità di un'interrogazione, di controllare la liceità del trattamento dei dati, dell'autocontrollo e di garantire il corretto funzionamento del CS-SIS, l'integrità e la sicurezza dei dati hanno accesso a tali registri, nei limiti delle rispettive competenze e su loro richiesta, ai fini dell'assolvimento dei loro doveri.

#### Articolo 19

##### **Campagna informativa**

La Commissione, in collaborazione con le autorità nazionali di controllo e con il garante europeo della protezione dei dati, lancia, in concomitanza con l'entrata in funzione del SIS II, una campagna informativa rivolta al pubblico sugli obiettivi, i dati memorizzati, le autorità che vi hanno accesso e i diritti delle persone. Una volta istituito, l'organo di gestione, in collaborazione con le autorità nazionali di controllo e con il garante europeo della protezione dei dati, ripete siffatte campagne a intervalli regolari. Gli Stati membri, in collaborazione con le autorità nazionali di controllo, definiscono e attuano le politiche necessarie per informare i propri cittadini sul SIS II in generale.

#### CAPO IV

##### **CATEGORIE DI DATI E INDICATORI DI VALIDITÀ**

#### Articolo 20

##### **Categorie di dati**

1. Fatti salvi l'articolo 8, paragrafo 1, o le disposizioni della presente decisione che prevedono la memorizzazione di dati complementari, il SIS II contiene esclusivamente le categorie di dati forniti da ciascuno Stato membro, come richiesto ai fini previsti negli articoli 26, 32, 34, 36 e 38.

2. Le categorie di dati sono le seguenti:

- a) le persone segnalate;
- b) gli oggetti di cui agli articoli 36 e 38.

3. Le informazioni sulle persone segnalate si limitano alle seguenti:

- a) cognomi e nomi, cognomi alla nascita, eventuali cognomi precedenti e «alias» che possono essere registrati a parte;
- b) segni fisici particolari, oggettivi ed inalterabili;
- c) luogo e data di nascita;
- d) sesso;
- e) fotografie;
- f) impronte digitali;
- g) cittadinanza(e);
- h) indicazione che la persona in questione è armata, violenta o è evasa;
- i) ragione della segnalazione;
- j) autorità che effettua la segnalazione;
- k) riferimento alla decisione che ha dato origine alla segnalazione;
- l) azione da intraprendere;

m) connessioni con altre segnalazioni già introdotte nel SIS II a norma dell'articolo 52;

n) tipo di reato.

4. Le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui ai paragrafi 2 e 3 sono stabilite secondo la procedura di cui all'articolo 67, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.

5. Le norme tecniche necessarie per la consultazione dei dati di cui al paragrafo 3 sono analoghe per le consultazioni nel CS-SIS, nelle copie nazionali e nelle copie tecniche, di cui all'articolo 46, paragrafo 2.

#### Articolo 21

##### Proporzionalità

Prima di effettuare una segnalazione lo Stato membro verifica se l'adeguatezza, la pertinenza e l'importanza del caso giustificano l'inserimento della segnalazione nel SIS II.

#### Articolo 22

##### Norme specifiche per fotografie e impronte digitali

L'uso di fotografie e impronte digitali di cui all'articolo 20, paragrafo 3, lettere e) ed f), è soggetto alle seguenti disposizioni:

- a) fotografie e impronte digitali possono essere inserite solo previo controllo speciale di qualità per accertare che soddisfino uno standard minimo di qualità dei dati. Le specifiche sul controllo speciale di qualità sono stabilite secondo la procedura di cui all'articolo 67, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione;
- b) fotografie e impronte digitali sono usate solo per confermare l'identità di una persona individuata grazie all'interrogazione del SIS II con dati alfanumerici;
- c) possono essere usate impronte digitali, non appena diventi possibile tecnicamente, anche per identificare una persona in base al suo identificatore biometrico. Prima che questa funzione sia attuata nel SIS II, la Commissione presenta una relazione sulla disponibilità e sullo stato di preparazione della tecnologia necessaria, in merito alla quale il Parlamento europeo è consultato.

#### Articolo 23

##### Requisito per inserire una segnalazione

1. Non si possono inserire segnalazioni su persone in mancanza dei dati di cui all'articolo 20, paragrafo 3, lettere a), d), l) e, ove applicabile, k).
2. Se disponibili, sono inseriti anche tutti gli altri dati di cui all'articolo 20, paragrafo 3.

#### Articolo 24

##### Disposizioni generali relative agli indicatori di validità

1. Qualora uno Stato membro reputi che dare applicazione ad una segnalazione inserita a norma degli articoli 26, 32 o 36 non sia compatibile con la legislazione nazionale, con i propri obblighi internazionali o con interessi nazionali essenziali, può esigere a posteriori che alla segnalazione sia apposto un indicatore di validità affinché non sia eseguita sul proprio territorio l'azione richiesta nella segnalazione. L'indicatore di validità è apposto dall'ufficio Sirene dello Stato membro che ha inserito la segnalazione.

2. Per consentire agli Stati membri di esigere l'apposizione di un indicatore di validità a una segnalazione effettuata a norma dell'articolo 26, tutti gli Stati membri sono automaticamente informati di ogni nuova segnalazione di questa categoria mediante lo scambio di informazioni supplementari.

3. Se per ragioni particolarmente gravi e urgenti lo Stato membro che ha emesso la segnalazione chiede l'esecuzione dell'azione, lo Stato membro che ha effettuato la segnalazione esamina se può acconsentire al ritiro dell'indicatore di validità di cui ha richiesto l'apposizione. Se vi può acconsentire, esso adotta le misure necessarie per far sì che l'azione richiesta sia eseguita immediatamente.

#### Articolo 25

##### Indicatori di validità relativi a segnalazioni per l'arresto a fini di consegna

1. Ove si applichi la decisione quadro 2002/584/GAI, l'indicatore di validità che impedisca l'arresto è apposto a una segnalazione per l'arresto a fini di consegna solo se l'autorità giudiziaria competente in virtù della legislazione nazionale per l'esecuzione del mandato di arresto europeo ne ha rifiutato l'esecuzione per motivi di non esecuzione e se l'apposizione dell'indicatore di validità è stata richiesta.

2. Tuttavia, su richiesta di un'autorità giudiziaria competente in virtù della legislazione nazionale, in base a un'istruzione generale o in un caso specifico, si può chiedere di apporre un indicatore di validità anche se risulta in modo evidente che l'esecuzione del mandato di arresto europeo dovrà essere rifiutata.

#### CAPO V

##### SEGNALAZIONE DI PERSONE RICERCATE PER L'ARRESTO A FINI DI CONSEGNA O DI ESTRADIZIONE

#### Articolo 26

##### Obiettivi e condizioni della segnalazione

1. I dati relativi alle persone ricercate per l'arresto a fini di consegna sulla scorta di un mandato d'arresto europeo, ovvero per l'arresto a fini di estradizione, sono inseriti su richiesta dell'autorità giudiziaria dello Stato membro della segnalazione.

2. I dati relativi alle persone ricercate per l'arresto a fini di consegna sono del pari inseriti sulla scorta di mandati di arresto emessi in conformità degli accordi conclusi tra l'Unione europea e i paesi terzi in virtù degli articoli 24 e 38 del trattato UE ai fini della consegna di persone sulla base di un mandato di arresto che prevedono la trasmissione di detto mandato di arresto mediante il sistema d'informazione Schengen.

#### Articolo 27

##### **Dati complementari su persone ricercate per l'arresto a fini di consegna**

1. Nel caso di persone ricercate per l'arresto a fini di consegna sulla scorta di un mandato d'arresto europeo, lo Stato membro della segnalazione inserisce nel SIS II una copia del mandato d'arresto europeo originale.

2. Lo Stato membro della segnalazione può inserire una copia della traduzione del mandato d'arresto europeo in una o più lingue ufficiali dell'Unione europea.

#### Articolo 28

##### **Informazioni supplementari su persone ricercate per l'arresto a fini di consegna**

Lo Stato membro che ha inserito la segnalazione nel SIS II per l'arresto a fini di consegna comunica le informazioni di cui all'articolo 8, paragrafo 1, della decisione quadro 2002/584/GAI a tutti gli Stati membri tramite lo scambio di informazioni supplementari.

#### Articolo 29

##### **Informazioni supplementari su persone ricercate per l'arresto a fini di estradizione**

1. Lo Stato membro che ha inserito la segnalazione nel SIS II a fini di estradizione comunica i dati seguenti a tutti gli Stati membri mediante lo scambio di informazioni supplementari:

- a) autorità da cui proviene la richiesta di arresto;
- b) esistenza di un mandato d'arresto o di un documento avente la medesima valenza giuridica, o di una sentenza esecutiva;
- c) natura e qualificazione giuridica del reato;
- d) descrizione delle circostanze in cui il reato è stato commesso, compreso il momento, il luogo ed il grado di partecipazione al reato della persona segnalata;
- e) per quanto possibile, le conseguenze del reato;
- f) qualsiasi altra informazione utile o necessaria per l'esecuzione della segnalazione.

2. I dati menzionati nel paragrafo 1 non sono comunicati se i dati di cui agli articoli 27 o 28 sono già stati forniti e sono considerati sufficienti per l'esecuzione della segnalazione dallo Stato membro interessato.

#### Articolo 30

##### **Conversione delle segnalazioni su persone ricercate per l'arresto a fini di consegna o di estradizione**

Se non è possibile procedere ad un arresto a causa di una decisione di rifiuto emessa da uno Stato membro richiesto secondo le procedure relative agli indicatori di validità di cui agli articoli 24 o 25 o, nel caso di una segnalazione per l'arresto a fini di estradizione, in quanto un'indagine non è ancora stata conclusa, lo Stato membro richiesto deve considerare la segnalazione come una segnalazione per comunicare il luogo di soggiorno della persona interessata.

#### Articolo 31

##### **Esecuzione dell'azione richiesta nella segnalazione di una persona ricercata per l'arresto in vista della consegna o dell'extradizione**

1. Una segnalazione inserita nel SIS II a norma dell'articolo 26 unitamente ai dati complementari di cui all'articolo 27 costituisce ed ha lo stesso effetto di un mandato d'arresto europeo emesso a norma della decisione quadro 2002/584/GAI, ove si applichi tale decisione quadro.

2. Ove non si applichi la decisione quadro 2002/584/GAI, una segnalazione inserita nel SIS II a norma degli articoli 26 e 29 ha la stessa valenza giuridica di una richiesta di arresto provvisorio a norma dell'articolo 16 della convenzione europea di estradizione del 13 dicembre 1957 o dell'articolo 15 del trattato di estradizione e di assistenza giudiziaria in materia penale tra il Regno del Belgio, il Granducato di Lussemburgo e il Regno dei Paesi Bassi, del 27 giugno 1962.

#### CAPO VI

##### **SEGNALAZIONE DI PERSONE SCOMPARSE**

#### Articolo 32

##### **Obiettivi e condizioni delle segnalazioni**

1. I dati relativi alle persone scomparse che devono essere poste sotto protezione e/o a quelle il cui luogo di soggiorno deve essere accertato sono inseriti nel SIS II su richiesta dell'autorità competente dello Stato membro che effettua la segnalazione.

2. Possono essere inserite le seguenti categorie di persone scomparse:

- a) persone scomparse che devono essere poste sotto protezione:
  - i) ai fini della loro tutela;
  - ii) per prevenire minacce;
- b) persone scomparse che non devono essere poste sotto protezione.

3. Il paragrafo 2, lettera a), si applica solo alle persone che devono essere internate per decisione di un'autorità competente.

4. I paragrafi 1, 2 e 3 si applicano in particolare ai minori.

5. Gli Stati membri assicurano che i dati inseriti nel SIS II indichino in quale delle categorie di cui al paragrafo 2 rientra la persona scomparsa.

#### Articolo 33

##### Esecuzione dell'azione richiesta nelle segnalazioni

1. In caso di individuazione di una persona di cui all'articolo 32, le autorità competenti comunicano, fatto salvo il paragrafo 2, il suo luogo di soggiorno allo Stato membro che effettua la segnalazione. Nei casi di cui all'articolo 32, paragrafo 2, lettera a), essa può, qualora la legislazione nazionale lo consenta, porre la suddetta persona sotto protezione per impedirle di proseguire il viaggio.

2. La comunicazione, diversa da quella fra le autorità competenti, dei dati di una persona scomparsa maggiorenne che sia stata individuata è subordinata al consenso della persona in questione. Tuttavia, le autorità competenti possono comunicare la cancellazione della segnalazione, dovuta alla localizzazione della persona, alla persona che ne ha segnalato la scomparsa.

#### CAPO VII

##### SEGNALAZIONE DI PERSONE RICERCATE PER PRESENZIARE AD UN PROCEDIMENTO GIUDIZIARIO

#### Articolo 34

##### Obiettivi e condizioni della segnalazione

Ai fini della comunicazione della residenza o del domicilio, gli Stati membri inseriscono nel SIS II, su richiesta dell'autorità competente, i dati relativi a:

- a) testimoni;
- b) persone citate a comparire o persone ricercate affinché si presentino dinanzi all'autorità giudiziaria nell'ambito di un procedimento penale per rispondere di fatti che sono loro ascritti;
- c) persone alle quali deve essere notificata una sentenza penale o altri documenti connessi con un procedimento penale per rispondere di fatti che sono stati loro ascritti;
- d) persone alle quali deve essere notificata una richiesta di presentarsi per scontare una pena privativa della libertà.

#### Articolo 35

##### Esecuzione dell'azione richiesta nelle segnalazioni

Le informazioni richieste sono comunicate allo Stato membro richiedente tramite scambio di informazioni supplementari.

#### CAPO VIII

##### SEGNALAZIONE DI PERSONE E OGGETTI AI FINI DI UN CONTROLLO DISCRETO O DI UN CONTROLLO SPECIFICO

#### Articolo 36

##### Obiettivi e condizioni della segnalazione

1. I dati relativi alle persone o a veicoli, natanti, aeromobili e container sono inseriti, nel rispetto della legislazione nazionale dello Stato membro che effettua la segnalazione, ai fini di un controllo discreto o di un controllo specifico, a norma dell'articolo 37, paragrafo 4.

2. Tale segnalazione può essere effettuata ai fini della repressione di reati e per prevenire minacce alla sicurezza pubblica:

- a) qualora esistano indizi concreti che una persona intenda commettere o commetta un reato grave, quali i reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI; oppure
- b) qualora la valutazione globale di una persona, in particolare sulla base dei reati commessi sino a quel momento, faccia supporre che commetterà anche in avvenire reati gravi, quali i reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI.

3. Inoltre, una segnalazione può essere effettuata conformemente alla legislazione nazionale, su richiesta delle autorità competenti per la sicurezza nazionale, qualora esistano indizi concreti che le informazioni di cui all'articolo 37, paragrafo 1, sono necessarie per prevenire una minaccia grave proveniente dall'interessato o altre minacce gravi per la sicurezza interna o esterna dello Stato. Lo Stato membro che effettua la segnalazione a norma del presente paragrafo ne informa gli altri Stati membri. Ciascuno Stato membro stabilisce a quali autorità sono trasmesse queste informazioni.

4. Le segnalazioni relative a veicoli, natanti, aeromobili e container possono essere effettuate qualora esistano indizi concreti che sono connesse con i reati gravi di cui al paragrafo 2 o con le minacce gravi di cui al paragrafo 3.

#### Articolo 37

##### Esecuzione dell'azione richiesta nelle segnalazioni

1. Nell'ambito del controllo discreto o del controllo specifico, le seguenti informazioni sono raccolte e trasmesse, totalmente o in parte, all'autorità che effettua la segnalazione, in occasione di controlli alla frontiera o di altri controlli di polizia e doganali effettuati all'interno di uno Stato membro:

- a) il fatto che siano stati individuati la persona o il veicolo, il natante, l'aeromobile o il container segnalati;
- b) il luogo, il momento o il motivo del controllo;

- c) l'itinerario e la destinazione del viaggio;
  - d) le persone che accompagnano gli interessati o gli occupanti del veicolo, del natante o dell'aeromobile di cui si può ragionevolmente presumere che siano associati agli interessati;
  - e) il veicolo, il natante, l'aeromobile o il container usato;
  - f) gli oggetti trasportati;
  - g) le circostanze in cui la persona o il veicolo, il natante, l'aeromobile o il container sono stati individuati.
- f) certificati di immatricolazione per veicoli e targhe di veicoli rubati, altrimenti sottratti, smarriti o falsificati;
  - g) banconote (banconote registrate);
  - h) valori mobiliari e mezzi di pagamento, quali assegni, carte di credito, obbligazioni, titoli e azioni, rubati, altrimenti sottratti, smarriti o falsificati.

2. Le informazioni di cui al paragrafo 1 sono trasmesse mediante lo scambio di informazioni supplementari.

3. Per la raccolta delle informazioni di cui al paragrafo 1, gli Stati membri provvedono affinché non sia compromesso il carattere discreto del controllo.

4. Nell'ambito dei controlli specifici, le persone, i veicoli, i natanti, gli aeromobili, i container e gli oggetti trasportati possono essere perquisiti conformemente alla legislazione nazionale, per i fini di cui all'articolo 36. Se la legge di uno Stato membro non lo autorizza, il controllo specifico viene automaticamente convertito, per quello Stato membro, in controllo discreto.

#### CAPO IX

##### SEGNALAZIONE DI OGGETTI A FINI DI SEQUESTRO O DI PROVA IN UN PROCEDIMENTO PENALE

###### Articolo 38

###### Obiettivi e condizioni della segnalazione

1. I dati relativi agli oggetti ricercati a scopo di sequestro o di prova in un procedimento penale sono inseriti nel SIS II.
2. Sono inserite le categorie di oggetti agevolmente identificabili indicate in appresso:
  - a) veicoli a motore di cilindrata superiore a 50 cc, natanti e aeromobili;
  - b) rimorchi di peso a vuoto superiore a 750 kg, roulotte, apparecchiature industriali, motori fuoribordo e container;
  - c) armi da fuoco;
  - d) documenti vergini rubati, altrimenti sottratti o smarriti;
  - e) documenti di identità rilasciati, quali passaporti, carte d'identità, patenti di guida, titoli di soggiorno e documenti di viaggio rubati, altrimenti sottratti, smarriti o falsificati;

3. Le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 2 sono stabilite secondo la procedura di cui all'articolo 67, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.

#### Articolo 39

##### Esecuzione dell'azione richiesta nelle segnalazioni

1. Qualora dall'interrogazione emerga l'esistenza di una segnalazione per un oggetto individuato, l'autorità che la constata si mette in contatto con l'autorità che ha effettuato la segnalazione per concordare le misure necessarie. A tale scopo, possono altresì essere trasmessi dati personali, a norma della presente decisione.
2. Le informazioni di cui al paragrafo 1 sono comunicate mediante lo scambio di informazioni supplementari.
3. Lo Stato membro che ha rinvenuto l'oggetto adotta misure conformi alla propria legislazione.

#### CAPO X

##### DIRITTO D'ACCESSO E CONSERVAZIONE DELLE SEGNALAZIONI

###### Articolo 40

###### Autorità con diritto di accesso alle segnalazioni

1. L'accesso ai dati inseriti nel SIS II e il diritto di consultarli direttamente o su una copia di dati del SIS II sono riservati esclusivamente alle autorità responsabili:
  - a) dei controlli di frontiera, a norma del regolamento (CE) n. 562/2006 del Parlamento europeo e del Consiglio, del 15 marzo 2006, che istituisce un codice comunitario relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen) <sup>(1)</sup>;
  - b) degli altri controlli di polizia e doganali effettuati all'interno dello Stato membro interessato e del relativo coordinamento da parte delle autorità designate.
2. Tuttavia, il diritto di accesso ai dati inseriti nel SIS II e il diritto di consultarli direttamente possono essere esercitati anche dalle autorità giudiziarie nazionali, comprese quelle responsabili dell'avvio dell'azione penale e delle indagini giudiziarie prima dell'imputazione, nell'assolvimento dei loro doveri, come previsto nella legislazione nazionale, e dalle relative autorità di coordinamento.

<sup>(1)</sup> GU L 105 del 13.4.2006, pag. 1.

3. Le autorità di cui al presente articolo sono inserite nell'elenco di cui all'articolo 46, paragrafo 8.

#### Articolo 41

##### Accesso dell'Europol ai dati SIS II

1. L'Ufficio europeo di polizia (Europol), nell'ambito del suo mandato, ha il diritto di accedere ai dati inseriti nel SIS II a norma degli articoli 26, 36 e 38 e di consultarli direttamente.

2. Qualora un'interrogazione effettuata dall'Europol riveli la presenza di una segnalazione nel SIS II, l'Europol, tramite i canali definiti dalla convenzione Europol, informa al riguardo lo Stato membro che ha effettuato la segnalazione.

3. L'uso delle informazioni ottenute tramite un'interrogazione nel SIS II è soggetto al consenso dello Stato membro interessato. Se lo Stato membro acconsente all'uso di tali informazioni, il loro trattamento è disciplinato dalla convenzione Europol. Le informazioni sono trasmesse dall'Europol a paesi terzi e organismi terzi solo con il consenso dello Stato membro interessato.

4. L'Europol, conformemente a quanto previsto dalla convenzione Europol, può chiedere ulteriori informazioni allo Stato membro interessato.

5. L'Europol:

- a) registra ogni accesso e interrogazione effettuati, secondo il disposto dell'articolo 12;
- b) fatti salvi i paragrafi 3 e 4, non collega le parti del SIS II né trasferisce i dati in esso contenuti cui ha accesso a sistemi informatici di raccolta ed elaborazione dei dati utilizzati dall'Europol o in funzione presso di esso e non scarica o copia altrimenti parti del SIS II;
- c) limita l'accesso ai dati inseriti nel SIS II a personale dell'Europol specificamente autorizzato;
- d) adotta ed applica le misure di cui agli articoli 10 e 11;
- e) consente all'autorità di controllo comune, istituita a norma dell'articolo 24 della convenzione Europol, di esaminare le attività dell'Europol nell'esercizio del suo diritto di accesso ai dati inseriti nel SIS II e di consultazione.

#### Articolo 42

##### Accesso dell'Eurojust ai dati SIS II

1. I membri nazionali dell'Eurojust e i loro assistenti, nell'ambito del loro mandato, hanno il diritto di accesso ai dati inseriti nel SIS II a norma degli articoli 26, 32, 34 e 38 e di consultazione.

2. Qualora un'interrogazione effettuata da un membro nazionale dell'Eurojust riveli la presenza di una segnalazione nel SIS II, il membro nazionale informa al riguardo lo Stato membro che ha effettuato la segnalazione. Qualsiasi informazione ottenuta a seguito di detta interrogazione può essere comunicata a paesi terzi e organismi terzi solo con il consenso dello Stato membro che ha effettuato la segnalazione.

3. È inteso che il presente articolo non pregiudica in alcun modo le disposizioni della decisione 2002/187/GAI concernenti la protezione dei dati e la responsabilità per eventuali trattamenti non autorizzati o scorretti di tali dati da parte dei membri nazionali dell'Eurojust o dei loro assistenti, né le competenze dell'autorità di controllo comune istituita a norma di detta decisione.

4. Ogni accesso e consultazione effettuati da un membro nazionale dell'Eurojust o da un assistente è registrata secondo il disposto dell'articolo 12 e ogni uso dei dati ai quali ha avuto accesso è registrato.

5. Nessuna parte del SIS II è collegata a sistemi informatici di raccolta ed elaborazione dei dati utilizzati dall'Eurojust o in funzione presso di esso né vi sono trasferiti i dati contenuti nel sistema cui hanno accesso i membri nazionali o i loro assistenti, e nessuna parte del SIS II viene scaricata.

6. L'accesso ai dati inseriti nel SIS II è limitato ai membri nazionali e ai loro assistenti e non si estende al personale dell'Eurojust.

7. Sono adottate e applicate le misure per garantire sicurezza e riservatezza di cui agli articoli 10 e 11.

#### Articolo 43

##### Ambito dell'accesso

Gli utenti, compreso l'Europol, i membri nazionali dell'Eurojust e i loro assistenti, possono accedere solo ai dati necessari per l'assolvimento dei loro compiti.

#### Articolo 44

##### Termini di conservazione delle segnalazioni relative a persone

1. Le segnalazioni relative alle persone inserite nel SIS II a norma della presente decisione sono conservate esclusivamente per il periodo necessario a realizzare gli obiettivi per i quali sono state inserite.

2. Uno Stato membro che ha effettuato una segnalazione riesamina la necessità di conservarla nel SIS II entro tre anni dall'inserimento nello stesso. Il periodo è ridotto a un anno per le segnalazioni relative alle persone di cui all'articolo 36.

3. Ciascuno Stato membro fissa, se del caso, tempi di riesame più brevi conformemente alla propria legislazione nazionale.

4. Nel periodo di riesame uno Stato membro che effettua la segnalazione può, a seguito di una valutazione individuale approfondita, decidere di mantenerla più a lungo, ove ciò sia necessario per gli scopi che sono alla base della segnalazione stessa. In tal caso il paragrafo 2 si applica anche a tale prolungamento. Ogni prolungamento di una segnalazione è comunicato al CS-SIS.

5. Le segnalazioni sono cancellate automaticamente allo scadere del periodo di riesame di cui al paragrafo 2, salvo qualora lo Stato membro che ha effettuato la segnalazione abbia comunicato il prolungamento della stessa al CS-SIS a norma del paragrafo 4. Il CS-SIS segnala automaticamente agli Stati membri, con quattro mesi d'anticipo, la prevista cancellazione di dati dal sistema.

6. Gli Stati membri tengono statistiche sul numero di segnalazioni il cui periodo di conservazione è stato prolungato a norma del paragrafo 4.

#### Articolo 45

##### **Termini di conservazione delle segnalazioni relative a oggetti**

1. Le segnalazioni relative ad oggetti inserite nel SIS II a norma della presente decisione sono conservate esclusivamente per il periodo necessario a realizzare gli obiettivi per i quali sono state inserite.

2. Le segnalazioni relative ad oggetti inserite a norma dell'articolo 36 sono conservate al massimo per cinque anni.

3. Le segnalazioni relative ad oggetti inserite a norma dell'articolo 38 sono conservate al massimo per dieci anni.

4. I termini di conservazione di cui ai paragrafi 2 e 3 possono essere prorogati, ove ciò sia necessario per gli scopi che sono alla base della segnalazione stessa. In tal caso, i paragrafi 2 e 3 si applicano anche alla proroga.

#### CAPO XI

##### **REGOLE GENERALI SUL TRATTAMENTO DEI DATI**

#### Articolo 46

##### **Trattamento dei dati SIS II**

1. Gli Stati membri possono trattare i dati di cui agli articoli 20, 26, 32, 34, 36 e 38 solo ai fini enunciati per ciascuna delle categorie di segnalazioni di cui a tali articoli.

2. I dati possono essere duplicati soltanto per fini tecnici, sempreché tale operazione sia necessaria per la consultazione diretta da parte delle autorità di cui all'articolo 40. Le disposizioni della presente decisione si applicano a tali copie. Le segnalazioni effettuate da uno Stato membro non possono essere copiate dal proprio N.SIS II in altri archivi di dati nazionali.

3. Le copie tecniche di cui al paragrafo 2 che portano alla creazione di banche dati off-line possono essere conservate solo per un periodo non superiore a quarantotto ore. Tale periodo può essere esteso in caso di emergenza, finché l'emergenza non sia cessata.

Gli Stati membri mantengono un inventario aggiornato di tali copie, lo rendono accessibile alle loro autorità nazionali di controllo e assicurano che le disposizioni della presente decisione, in particolare quelle dell'articolo 10, vengano applicate a tali copie.

4. L'accesso ai dati è autorizzato esclusivamente nei limiti delle competenze delle autorità nazionali di cui all'articolo 40 e riservato al personale debitamente autorizzato.

5. Per quanto riguarda le segnalazioni di cui agli articoli 26, 32, 34, 36 e 38 della presente decisione, ogni trattamento delle informazioni in esse contenute per fini diversi da quelli per i quali sono state inserite nel SIS II deve essere connesso a un caso specifico e giustificato dalla necessità di prevenire una minaccia grave imminente per l'ordine pubblico e la sicurezza pubblica, per fondati motivi di sicurezza nazionale o ai fini della prevenzione di un reato grave. A tale scopo deve essere ottenuta l'autorizzazione preventiva dello Stato membro che effettua la segnalazione.

6. I dati non possono essere usati a scopi amministrativi.

7. Qualsiasi uso dei dati non conforme ai paragrafi da 1 a 6 è considerato un uso illegale ai sensi della legislazione di ciascuno Stato membro.

8. Ciascuno Stato membro invia all'organo di gestione un elenco delle proprie autorità competenti autorizzate a consultare direttamente i dati inseriti nel SIS II a norma della presente decisione e delle eventuali modifiche apportate all'elenco. L'elenco indica per ciascuna autorità i dati che essa può consultare e a quali fini. L'organo di gestione provvede alla pubblicazione annuale dell'elenco nella *Gazzetta ufficiale dell'Unione europea*.

9. Sempreché il diritto dell'Unione europea non preveda disposizioni particolari, la legislazione di ciascuno Stato membro si applica ai dati inseriti nel rispettivo N.SIS II.

#### Articolo 47

##### **Dati SIS II e archivi nazionali**

1. L'articolo 46, paragrafo 2, non pregiudica il diritto di uno Stato membro di conservare nel proprio archivio nazionale i dati SIS II in collegamento con i quali è stata svolta un'azione nel suo territorio. Tali dati sono conservati negli archivi nazionali per un periodo massimo di tre anni, a meno che disposizioni specifiche di diritto nazionale prevedano un periodo di conservazione più lungo.

2. L'articolo 46, paragrafo 2, non pregiudica il diritto di uno Stato membro di conservare nel proprio archivio nazionale i dati contenuti in una segnalazione particolare effettuata nel SIS II da quello stesso Stato membro.



*Articolo 48***Informazione in caso di mancata esecuzione di una segnalazione**

Se l'azione richiesta non può essere eseguita, lo Stato membro a cui è stata presentata la richiesta ne informa senza indugio lo Stato membro che ha effettuato la segnalazione.

*Articolo 49***Qualità dei dati trattati nel SIS II**

1. Uno Stato membro che effettua una segnalazione è responsabile dell'esattezza, dell'attualità e della liceità di inserimento dei dati nel SIS II.

2. Solo lo Stato membro che ha effettuato una segnalazione è autorizzato a modificare, completare, rettificare, aggiornare o cancellare i dati che ha inserito.

3. Se uno Stato membro diverso da quello che ha effettuato una segnalazione è in possesso di elementi che dimostrano che detti dati contengono errori di fatto o sono stati archiviati illecitamente, ne informa quanto prima, tramite scambio di informazioni supplementari ed entro dieci giorni dacché è in possesso di detti elementi, lo Stato membro che ha effettuato la segnalazione. Quest'ultimo verifica la comunicazione e, se necessario, rettifica o cancella senza indugio i dati in questione.

4. Se entro due mesi gli Stati membri non giungono a un accordo, lo Stato membro che non ha effettuato la segnalazione sottopone la questione al garante europeo della protezione dei dati, il quale, insieme alle autorità nazionali di controllo interessate, agisce in qualità di mediatore.

5. Gli Stati membri si scambiano informazioni supplementari se una persona presenta un ricorso nel quale fa valere di non essere la persona oggetto della segnalazione. Se dalla verifica risulta che si tratta in effetti di due persone distinte, il ricorrente è informato delle disposizioni dell'articolo 51.

6. Se una persona è già segnalata nel SIS II, lo Stato membro che introduce un'altra segnalazione si accorda in merito a tale inserimento con lo Stato membro che ha effettuato la prima segnalazione. L'accordo è raggiunto sulla base allo scambio di informazioni supplementari.

*Articolo 50***Distinzione tra persone con caratteristiche simili**

Quando, inserendo una nuova segnalazione, risulta evidente che nel SIS II è già registrata una persona che possiede gli stessi elementi di descrizione dell'identità, occorre seguire la procedura seguente:

a) l'ufficio Sirene si mette in contatto con l'autorità richiedente allo scopo di verificare se la segnalazione riguarda o meno la stessa persona;

b) se da tale controllo incrociato risulta che la persona oggetto di una nuova segnalazione e la persona già registrata nel SIS II sono la stessa, l'ufficio Sirene applica la procedura per l'inserimento di segnalazioni multiple di cui all'articolo 49, paragrafo 6. Qualora si stabilisca che si tratta di due persone diverse, l'ufficio Sirene convalida la richiesta di inserimento della seconda segnalazione aggiungendo gli elementi necessari per evitare errori di identificazione.

*Articolo 51***Dati complementari per trattare i casi di usurpazione di identità**

1. Quando sono possibili confusioni fra la persona effettivamente oggetto di una segnalazione e una persona la cui identità è stata usurpata, lo Stato membro che ha introdotto la segnalazione vi aggiunge, con il consenso esplicito della persona interessata, dati che la riguardano per evitare le conseguenze negative di un errore di identificazione.

2. I dati relativi alla vittima dell'usurpazione di identità sono usati soltanto ai seguenti fini:

a) consentire all'autorità competente di distinguere la persona la cui identità è stata usurpata dalla persona effettivamente oggetto della segnalazione;

b) permettere alla persona la cui identità è stata usurpata di dimostrare la propria identità e stabilire di essere stata vittima di un'usurpazione di identità.

3. Ai fini del presente articolo possono essere inseriti e successivamente trattati nel SIS II solo i seguenti dati personali:

a) cognomi e nomi, cognomi alla nascita, eventuali cognomi precedenti e «alias» eventualmente registrati a parte;

b) segni fisici particolari, oggettivi ed inalterabili;

c) luogo e data di nascita;

d) sesso;

e) fotografie;

f) impronte digitali;

g) cittadinanza(e);

h) numero del o dei documenti d'identità e data del rilascio.

4. Le norme tecniche necessarie per l'inserimento e l'ulteriore trattamento dei dati di cui al paragrafo 3 sono stabilite secondo la procedura di cui all'articolo 67, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.

5. I dati di cui al paragrafo 3 sono cancellati insieme con la segnalazione corrispondente o prima su richiesta dell'interessato.

6. Possono accedere ai dati di cui al paragrafo 3 soltanto le autorità che hanno diritto di accesso alla segnalazione corrispondente e all'unico scopo di evitare errori di identificazione.

#### Articolo 52

### Connessioni fra segnalazioni

1. Uno Stato membro può creare una connessione tra le segnalazioni che introduce nel SIS II. Effetto della connessione è istaurare un nesso fra due o più segnalazioni.

2. La creazione di una connessione non incide sulla specifica azione da intraprendere sulla base di ciascuna segnalazione interconnessa né sul rispettivo termine di conservazione.

3. La creazione di una connessione non incide sui diritti di accesso previsti nella presente decisione. Le autorità che non hanno diritto di accesso a talune categorie di segnalazioni non sono in grado di visualizzare la connessione a una segnalazione cui non hanno accesso.

4. Uno Stato membro crea una connessione tra segnalazioni solo se sussiste una reale esigenza operativa.

5. Uno Stato membro può creare connessioni conformemente alla legislazione nazionale purché siano rispettati i principi enunciati nel presente articolo.

6. Uno Stato membro, qualora ritenga che la creazione di una connessione tra segnalazioni da parte di un altro Stato membro sia incompatibile con la sua legislazione nazionale o i suoi obblighi internazionali, può adottare le necessarie disposizioni affinché non sia possibile accedere alla connessione dal suo territorio nazionale o per le sue autorità dislocate al di fuori del suo territorio.

7. Le norme tecniche per la connessione delle segnalazioni sono adottate secondo la procedura di cui all'articolo 67, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.

#### Articolo 53

### Finalità e termini di conservazione delle informazioni supplementari

1. Gli Stati membri conservano un riferimento alle decisioni di effettuare una segnalazione presso l'ufficio Sirene, a sostegno dello scambio di informazioni supplementari.

2. I dati personali archiviati dall'ufficio Sirene in seguito allo scambio di informazioni sono conservati soltanto per il tempo necessario a conseguire gli scopi per i quali sono stati forniti. Essi sono in ogni caso cancellati al più tardi un anno dopo che è stata cancellata dal SIS II la relativa segnalazione.

3. Il paragrafo 2 non pregiudica il diritto di uno Stato membro di conservare negli archivi nazionali i dati relativi ad una determinata segnalazione effettuata da detto Stato membro o ad una segnalazione in collegamento con la quale è stata intrapresa un'azione nel suo territorio. Il periodo per cui tali dati possono essere conservati in tali archivi è regolato dalla legislazione nazionale.

#### Articolo 54

### Trasferimento di dati personali a terzi

I dati trattati nel SIS II a norma della presente decisione non sono trasferiti a paesi terzi o a organizzazioni internazionali, né sono messi a loro disposizione.

#### Articolo 55

### Scambio di dati con l'Interpol sui passaporti rubati, altrimenti sottratti, smarriti o falsificati

1. In deroga all'articolo 54 il numero, il paese di rilascio e la tipologia dei passaporti rubati, altrimenti sottratti, smarriti o falsificati inseriti nel SIS II possono essere scambiati con membri dell'Interpol stabilendo un collegamento tra il SIS II e la banca dati dell'Interpol sui documenti di viaggio rubati o smarriti, fatta salva la conclusione di un accordo tra l'Interpol e l'Unione europea. In base a tale accordo la trasmissione di dati inseriti da uno Stato membro è soggetta al consenso di tale Stato membro.

2. L'accordo di cui al paragrafo 1 prevede che i dati condivisi siano accessibili solo a membri dell'Interpol di paesi che assicurano un adeguato livello di protezione dei dati personali. Prima di concludere l'accordo, il Consiglio chiede il parere della Commissione sull'adeguatezza del livello di protezione dei dati personali e di rispetto dei diritti e delle libertà fondamentali per quanto riguarda il trattamento automatizzato dei dati personali da parte dell'Interpol e da parte dei paesi che hanno distaccato membri presso l'Interpol.

3. L'accordo di cui al paragrafo 1 può anche prevedere che gli Stati membri abbiano accesso, attraverso il SIS II, ai dati della banca dati dell'Interpol sui documenti di viaggio rubati o smarriti, in conformità delle pertinenti disposizioni della presente decisione che disciplinano le segnalazioni sui passaporti rubati, altrimenti sottratti, smarriti o falsificati inserite nel SIS II.

## CAPO XII

**PROTEZIONE DEI DATI***Articolo 56***Trattamento di categorie di dati sensibili**

È vietato il trattamento delle categorie di dati elencati nell'articolo 6, prima frase, della convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale.

*Articolo 57***Applicazione della convenzione del Consiglio d'Europa sulla protezione dei dati**

I dati personali trattati in applicazione della presente decisione sono protetti a norma della convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, e successive modifiche.

*Articolo 58***Diritto di accesso, rettifica di dati inesatti e cancellazione di dati archiviati illecitamente**

1. Il diritto di una persona di accedere ai dati che la riguardano inseriti nel SIS II conformemente alla presente decisione è esercitato nel rispetto della legislazione dello Stato membro presso il quale l'interessato lo fa valere.
2. Ove previsto dalla legislazione nazionale, l'autorità nazionale di controllo decide se ed in base a quali modalità deve comunicare informazioni.
3. Uno Stato membro diverso da quello che ha effettuato una segnalazione può comunicare informazioni su tali dati soltanto se dà prima la possibilità allo Stato membro che ha effettuato la segnalazione di prendere posizione. A ciò si provvede tramite lo scambio di informazioni supplementari.
4. L'informazione non è comunicata alla persona interessata se ciò è indispensabile per l'esecuzione di un compito legittimo connesso con una segnalazione o ai fini della tutela dei diritti e delle libertà di terzi.
5. Chiunque ha il diritto di far rettificare dati che lo riguardano contenenti errori di fatto o di far cancellare dati che lo riguardano inseriti illecitamente.
6. L'interessato è informato prima possibile e comunque non oltre 60 giorni dalla data in cui ha chiesto l'accesso o prima, se la legislazione nazionale lo prevede.

7. L'interessato è informato del seguito dato all'esercizio del suo diritto di rettifica e cancellazione prima possibile e comunque non oltre tre mesi dalla data in cui ha chiesto la rettifica o la cancellazione o prima, se la legislazione nazionale lo prevede.

*Articolo 59***Mezzi di impugnazione**

1. Chiunque può adire la giurisdizione o l'autorità competente in base alla legislazione di qualsiasi Stato membro per accedere, rettificare, cancellare o ottenere informazioni o per ottenere un indennizzo relativamente ad una segnalazione che lo riguarda.
2. Gli Stati membri si impegnano reciprocamente ad eseguire le decisioni definitive emesse dalle giurisdizioni o dalle autorità di cui al paragrafo 1, fatte salve le disposizioni dell'articolo 64.
3. La Commissione valuta le norme sui mezzi di impugnazione di cui al presente articolo entro il 23 agosto 2009.

*Articolo 60***Controllo dell'N.SIS II**

1. Ciascuno Stato membro provvede affinché un'autorità indipendente (l'«autorità nazionale di controllo») controlli autonomamente la liceità del trattamento dei dati personali SIS II nel loro territorio e della loro trasmissione dal loro territorio, compresi lo scambio e il successivo trattamento di informazioni supplementari.
2. L'autorità nazionale di controllo provvede affinché venga svolto un controllo delle operazioni di trattamento dei dati nel proprio N.SIS II, conformemente alle norme di revisione internazionali almeno ogni quattro anni.
3. Gli Stati membri provvedono affinché la propria autorità di controllo disponga delle risorse sufficienti per assolvere i compiti ad essa assegnati a norma della presente decisione.

*Articolo 61***Controllo dell'organo di gestione**

1. Il garante europeo della protezione dei dati controlla che le attività di trattamento dei dati personali dell'organo di gestione siano effettuate a norma della presente decisione. Si applicano di conseguenza i doveri e i poteri di cui agli articoli 46 e 47 del regolamento (CE) n. 45/2001.
2. Il garante europeo della protezione dei dati provvede affinché venga svolto un controllo delle attività di trattamento dei dati personali effettuate dall'organo di gestione, conformemente alle norme di revisione internazionali almeno ogni quattro anni. Una relazione su tale controllo è trasmessa al Parlamento europeo, al Consiglio, all'organo di gestione, alla Commissione e alle autorità nazionali di controllo. L'organo di gestione ha l'opportunità di presentare le sue osservazioni prima dell'adozione della relazione.

*Articolo 62***Cooperazione tra le autorità nazionali di controllo e il garante europeo della protezione dei dati**

1. Le autorità nazionali di controllo e il garante europeo della protezione dei dati, ciascuno nell'ambito delle proprie competenze, cooperano attivamente nel quadro delle rispettive responsabilità e assicurano il controllo coordinato del SIS II.

2. Se necessario, ciascuno nell'ambito delle proprie competenze, essi si scambiano informazioni pertinenti, si assistono reciprocamente nello svolgimento di revisioni e ispezioni, esaminano difficoltà di interpretazione o applicazione della presente decisione, studiano problemi inerenti all'esercizio di un controllo indipendente o all'esercizio dei diritti delle persone cui i dati si riferiscono, elaborano proposte armonizzate per soluzioni congiunte di eventuali problemi e promuovono la sensibilizzazione del pubblico in materia di diritti di protezione dei dati.

3. Le autorità nazionali di controllo e il garante europeo della protezione dei dati si riuniscono a tal fine almeno due volte l'anno. I costi di tali riunioni e la gestione delle stesse sono a carico del garante europeo della protezione dei dati. Nella prima riunione è adottato un regolamento interno. Ulteriori metodi di lavoro sono elaborati congiuntamente, se necessario. Ogni due anni è trasmessa al Parlamento europeo, al Consiglio, alla Commissione e all'organo di gestione una relazione congiunta sulle attività svolte.

*Articolo 63***Protezione dei dati durante il periodo transitorio**

La Commissione, qualora durante il periodo transitorio deleghi le sue competenze ad un altro organismo o ad altri organismi, a norma dell'articolo 15, paragrafo 4, provvede affinché il garante europeo della protezione dei dati abbia la facoltà e sia in grado di svolgere pienamente i suoi compiti, compresa l'effettuazione di controlli in loco o l'esercizio dei poteri attribuitigli dall'articolo 47 del regolamento (CE) n. 45/2001.

## CAPO XIII

**RESPONSABILITÀ E SANZIONI***Articolo 64***Responsabilità**

1. Ciascuno Stato membro è responsabile, conformemente alla propria legislazione nazionale, dei danni causati ad una persona in seguito all'uso dell'N.SIS II. La disposizione si applica anche quando i danni sono stati causati dallo Stato membro che ha effettuato la segnalazione, ove abbia inserito dati contenenti errori di fatto o archiviato i dati in modo illecito.

2. Se lo Stato membro avverso il quale è promossa un'azione non è lo Stato membro che ha effettuato la segnalazione, quest'ultimo è tenuto al rimborso, su richiesta, delle somme versate a titolo di risarcimento, a meno che l'uso dei dati da parte dello Stato membro che ha chiesto il rimborso violi la presente decisione.

3. Se l'inosservanza da parte di uno Stato membro degli obblighi derivanti dalla presente decisione causa danni al SIS II, tale Stato membro ne risponde, a meno che e nella misura in cui l'organo di gestione o un altro Stato membro partecipanti al SIS II non abbiano ommesso di adottare le misure ragionevolmente necessarie a evitare tali danni o a minimizzarne gli effetti.

*Articolo 65***Sanzioni**

Gli Stati membri provvedono affinché l'eventuale uso improprio dei dati inseriti nel SIS II o qualsiasi scambio di informazioni supplementari contrario alla presente decisione sia punito con sanzioni effettive, proporzionate e dissuasive conformemente alla legislazione nazionale.

## CAPO XIV

**DISPOSIZIONI FINALI***Articolo 66***Controllo e statistiche**

1. L'organo di gestione provvede affinché siano attivate procedure atte a controllare il funzionamento del SIS II in rapporto a obiettivi di risultato, economicità, sicurezza e qualità del servizio.

2. Ai fini della manutenzione tecnica, delle relazioni e delle statistiche, l'organo di gestione ha accesso alle informazioni necessarie riguardanti le operazioni di trattamento effettuate nel SIS II centrale.

3. Ogni anno l'organo di gestione pubblica statistiche, sia totali sia per ciascuno Stato membro, relative al numero di registri per categoria di segnalazione, al numero di risposte positive per categoria di segnalazione e al numero di accessi al SIS II.

4. Due anni dopo l'inizio delle attività del SIS II e successivamente ogni due anni, l'organo di gestione presenta al Parlamento europeo e al Consiglio una relazione sul funzionamento tecnico del SIS II centrale e dell'infrastruttura di comunicazione, compresa la sicurezza dello stesso e lo scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri.

5. Tre anni dopo l'inizio delle attività del SIS II e successivamente ogni quattro anni, la Commissione presenta una valutazione globale del SIS II centrale e dello scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri. Tale valutazione globale comprende un'analisi dei risultati conseguiti rispetto agli obiettivi e una valutazione circa la validità dei principi di base, l'applicazione della presente decisione con riguardo al SIS II centrale, la sicurezza del SIS II centrale e le eventuali implicazioni per le attività future. La Commissione trasmette la valutazione al Parlamento europeo e al Consiglio.

6. Gli Stati membri comunicano all'organo di gestione e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 3, 4 e 5.

7. L'organo di gestione comunica alla Commissione le informazioni necessarie per presentare le valutazioni globali di cui al paragrafo 5.

#### Articolo 67

##### Comitato di regolamentazione

1. Nei casi in cui è fatto riferimento al presente articolo, la Commissione è assistita da un comitato di regolamentazione composto dai rappresentanti degli Stati membri e presieduto dal rappresentante della Commissione. Il rappresentante della Commissione sottopone al comitato un progetto delle misure da adottare. Il comitato esprime il suo parere sul progetto entro un termine che il presidente può fissare in funzione dell'urgenza della questione in esame. Il parere è formulato alla maggioranza prevista all'articolo 205, paragrafo 2, del trattato CE per l'adozione delle decisioni che il Consiglio deve prendere su proposta della Commissione. Nelle votazioni del comitato, ai voti dei rappresentanti degli Stati membri è attribuita la ponderazione definita in quell'articolo. Il presidente non partecipa al voto.

2. Il comitato adotta il proprio regolamento interno su proposta del presidente, basandosi su un modello di regolamento interno pubblicato nella *Gazzetta ufficiale dell'Unione europea*.

3. La Commissione adotta le misure previste qualora siano conformi al parere del comitato. Se le misure previste non sono conformi al parere del comitato, o in assenza di parere, la Commissione sottopone senza indugio al Consiglio una proposta in merito alle misure da adottare.

4. Il Consiglio può deliberare sulla proposta a maggioranza qualificata entro due mesi dalla data in cui gli è stata presentata la proposta. Se entro tale termine il Consiglio ha manifestato a maggioranza qualificata la sua opposizione alla proposta, la Commissione la riesamina. Essa può presentare al Consiglio una proposta modificata, ripresentare la proposta ovvero presentare una proposta legislativa. Se allo scadere di tale termine il Consiglio non ha adottato l'atto di esecuzione proposto ovvero non ha manifestato opposizione alla proposta di misure di esecuzione, la Commissione adotta l'atto di esecuzione proposto.

5. Il comitato di cui al paragrafo 1 esercita la sua funzione a partire dal 23 agosto 2007.

#### Articolo 68

##### Modifica delle disposizioni dell'acquis di Schengen

1. Per le materie che rientrano nell'ambito di applicazione del trattato UE, la presente decisione sostituisce, alla data di cui all'articolo 71, paragrafo 2, le disposizioni degli articoli 64 e da 92 a 119 della convenzione di Schengen, salvo l'articolo 102 bis.

2. Per le materie che rientrano nell'ambito di applicazione del trattato UE, la presente decisione sostituisce, alla data di cui

all'articolo 71, paragrafo 2, le seguenti disposizioni dell'acquis di Schengen che attuano quegli articoli <sup>(1)</sup>:

- a) decisione del comitato esecutivo, del 14 dicembre 1993, relativa al regolamento finanziario riguardante le spese relative all'installazione e al funzionamento del sistema d'informazione Schengen (C.SIS) [SCH/Com-ex (93) 16];
- b) decisione del comitato esecutivo, del 7 ottobre 1997, riguardante l'evoluzione del SIS [SCH/Com-ex (97) 24];
- c) decisione del comitato esecutivo, del 15 dicembre 1997, riguardante la modifica del regolamento finanziario C.SIS [SCH/Com-ex (97) 35];
- d) decisione del comitato esecutivo, del 21 aprile 1998, riguardante il C.SIS con 15/18 collegamenti [SCH/Com-ex (98) 11];
- e) decisione del comitato esecutivo, del 25 aprile 1997, relativa all'aggiudicazione dello studio preliminare del SIS II [SCH/Com-ex (97) 2, rev. 2];
- f) decisione del comitato esecutivo, del 28 aprile 1999, riguardante i costi d'installazione del C.SIS [SCH/Com-ex (99) 4];
- g) decisione del comitato esecutivo, del 28 aprile 1999, riguardante l'aggiornamento del manuale Sirene [SCH/Com-ex (99) 5];
- h) dichiarazione del comitato esecutivo, del 18 aprile 1996, relativa alla definizione del concetto di straniero [SCH/Com-ex (96) decl. 5];
- i) dichiarazione del comitato esecutivo, del 28 aprile 1999, riguardante la struttura del SIS [SCH/Com-ex (99) decl. 2 rev.];
- j) decisione del comitato esecutivo, del 7 ottobre 1997, riguardante il contributo della Norvegia e dell'Islanda alle spese d'installazione e di funzionamento del C.SIS [SCH/Com-ex (97) 18].

3. Per le materie che rientrano nell'ambito di applicazione del trattato UE, i riferimenti agli articoli della convenzione di Schengen così sostituiti e alle pertinenti disposizioni dell'acquis di Schengen che li attuano si intendono fatti alla presente decisione.

#### Articolo 69

##### Abrogazione

Alla data di cui all'articolo 71, paragrafo 2, sono abrogate le decisioni 2004/201/GAI, 2005/211/GAI, 2005/719/GAI, 2005/727/GAI, 2006/228/GAI, 2006/229/GAI e 2006/631/GAI.

<sup>(1)</sup> GU L 239 del 22.9.2000, pag. 439.

## Articolo 70

**Periodo transitorio e bilancio**

1. Le segnalazioni sono trasferite dal SIS 1+ al SIS II. Gli Stati membri assicurano, attribuendo la priorità alle segnalazioni di persone, che il contenuto delle segnalazioni trasferite dal SIS 1+ al SIS II sia conforme alle disposizioni della presente decisione prima possibile e al più tardi entro tre anni dalla data di cui all'articolo 71, paragrafo 2. Nel periodo transitorio gli Stati membri possono continuare ad applicare gli articoli 94, 95 e da 97 a 100 della convenzione di Schengen al contenuto delle segnalazioni trasferite dal SIS 1+ al SIS II, fatte salve le seguenti regole:

- a) in caso di modifica, complemento, rettifica o aggiornamento del contenuto di una segnalazione trasferita dal SIS 1+ al SIS II, gli Stati membri assicurano che la segnalazione sia conforme alle disposizioni della presente decisione a decorrere dall'introduzione della modifica, complemento, rettifica o aggiornamento in questione;
- b) in caso di risposta positiva su una segnalazione trasferita dal SIS 1+ al SIS II, gli Stati membri esaminano immediatamente la compatibilità di tale segnalazione con le disposizioni della presente decisione senza tuttavia ritardare l'azione da intraprendere in base alla stessa.

2. Alla data fissata a norma dell'articolo 71, paragrafo 2, il residuo del bilancio approvato in conformità delle disposizioni dell'articolo 119 della convenzione di Schengen è restituito agli Stati membri. Gli importi da restituire sono calcolati in base ai contributi degli Stati membri in conformità della decisione del comitato esecutivo, del 14 dicembre 1993, relativa al regolamento finanziario riguardante le spese relative all'installazione e al funzionamento del SIS.

3. Durante il periodo transitorio di cui all'articolo 15, paragrafo 4, i riferimenti, nella presente decisione, all'organo di gestione si intendono fatti alla Commissione.

## Articolo 71

**Entrata in vigore, applicabilità e migrazione**

1. La presente decisione entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. Essa si applica agli Stati membri partecipanti al SIS 1+ a partire dalle date che il Consiglio stabilirà, deliberando all'unanimità dei suoi membri che rappresentano i governi degli Stati membri partecipanti al SIS 1+.

3. Le date di cui al paragrafo 2 sono stabilite:

- a) una volta adottate le necessarie disposizioni di attuazione;
- b) quando tutti gli Stati membri partecipanti a pieno titolo al SIS 1+ avranno notificato alla Commissione di aver adottato le disposizioni tecniche e giuridiche necessarie per trattare i dati SIS II e scambiare informazioni supplementari;
- c) quando la Commissione avrà dichiarato che è stato ultimato con esito positivo un test globale del SIS II, condotto dalla Commissione con gli Stati membri, e gli organi preparatori del Consiglio avranno convalidato i risultati proposti del test e confermato che il livello di prestazione del SIS II è almeno equivalente a quello già garantito dal SIS 1+;
- d) quando la Commissione avrà adottato le necessarie disposizioni tecniche per consentire la connessione del SIS II centrale all'N.SIS II degli Stati membri interessati.

4. La Commissione comunica al Parlamento europeo i risultati del test condotto a norma del paragrafo 3, lettera c).

5. Qualsiasi decisione del Consiglio presa ai sensi del paragrafo 2 è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Lussemburgo, addì 12 giugno 2007.

Per il Consiglio  
Il presidente  
W. SCHÄUBLE