

Il presente testo è un semplice strumento di documentazione e non produce alcun effetto giuridico. Le istituzioni dell'Unione non assumono alcuna responsabilità per i suoi contenuti. Le versioni facenti fede degli atti pertinenti, compresi i loro preamboli, sono quelle pubblicate nella Gazzetta ufficiale dell'Unione europea e disponibili in EUR-Lex. Tali testi ufficiali sono direttamente accessibili attraverso i link inseriti nel presente documento

► **B** **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)

(GU L 381 del 28.12.2006, pag. 4)

Modificato da:

| | | Gazzetta ufficiale | | |
|--------------------|--|--------------------|------|------------|
| | | n. | pag. | data |
| ► <u>M1</u> | Regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio del 14 novembre 2018 | L 295 | 99 | 21.11.2018 |
| ► <u>M2</u> | Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio del 28 novembre 2018 | L 312 | 14 | 7.12.2018 |

Rettificato da:

► **C1** Rettifica, GU L 23 del 29.1.2015, pag. 19 (1987/2006)



**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)**

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 del presente regolamento, assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione europea, incluso il mantenimento 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 relativo alla circolazione delle persone in detto territorio avvalendosi delle informazioni trasmesse tramite tale sistema.

Articolo 2

Ambito di applicazione

1. Il presente regolamento stabilisce le condizioni e le procedure applicabili all'inserimento e al trattamento nel SIS II delle segnalazioni relative a cittadini di paesi terzi, allo scambio di informazioni supplementari e dati complementari ai fini del rifiuto d'ingresso o di soggiorno nello Stato membro.
2. Il presente regolamento 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

Ai fini del presente regolamento, si intende per:

- a) «segnalazione»: un insieme di dati inseriti nel SIS II che permetta alle autorità competenti di identificare un individuo 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;

▼B

- 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 localizzata grazie all'interrogazione di tale sistema;
- d) «cittadino di paese terzo»: chi non è
- i) né cittadino dell'Unione europea ai sensi dell'articolo 17, paragrafo 1 del trattato;
 - ii) né cittadino di un paese terzo che, ai sensi di accordi conclusi tra la Comunità e i suoi Stati membri, da un lato, e il paese in questione, dall'altro, gode di diritti in materia di libera circolazione equivalenti a quelli dei cittadini dell'Unione europea;
- e) «dati personali»: qualsiasi informazione concernente una persona fisica identificata o identificabile («una persona interessata»); una persona identificabile è una persona che può essere identificata direttamente o indirettamente;
- f) «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.

*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

- 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 («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, che 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.

▼B

CAPO II

COMPETENZE DEGLI STATI MEMBRI**▼M2***Articolo 6***Sistemi nazionali**

1. Ciascuno Stato membro è competente per l'istituzione, l'esercizio, la manutenzione e l'ulteriore sviluppo del proprio N.SIS II e per il suo collegamento all'NI-SIS.
2. Ciascuno Stato membro è responsabile di garantire la disponibilità ininterrotta dei dati SIS II agli utenti finali.

▼B*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 del presente regolamento. 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 31, 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 securizzati per lo scambio di informazioni supplementari.
2. Le informazioni supplementari sono usate solo per lo scopo per il quale sono state trasmesse.

▼B

3. Alle richieste di informazioni supplementari formulate da uno Stato membro 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 51, paragrafo 2 sotto forma del 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 51, paragrafo 2, 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, costantemente 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);

▼B

- 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 descrivano 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 44, paragrafo 1 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 o durante il 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 del presente regolamento (autocontrollo).
2. Gli Stati membri adottano misure equivalenti a quelle del paragrafo 1 per quanto riguarda la sicurezza degli scambi di informazioni supplementari.

▼M2*Articolo 11***Riservatezza – Stati membri**

1. 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.

▼ M2

2. Se collabora con contraenti esterni per un qualsiasi compito relativo al SIS II, lo Stato membro monitora da vicino le attività del contraente per garantire il rispetto di tutte le disposizioni del presente regolamento, in particolare sulla sicurezza, la riservatezza e la protezione dei dati.

3. La gestione operativa dell'N.SIS II o delle copie tecniche non può essere affidata a imprese o organizzazioni private.

▼ B*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 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 delle interrogazioni, di controllare la liceità del trattamento dei dati, dell'autocontrollo e di garantire il corretto funzionamento dell'NSIS 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.

▼B*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 del presente regolamento 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.

▼M1

2. L'organo di gestione è responsabile di tutti i compiti connessi con l'infrastruttura di comunicazione, in particolare:

- a) controllo;
- b) sicurezza;
- c) coordinamento dei rapporti tra gli Stati membri e il gestore;
- d) compiti relativi all'esecuzione del bilancio;
- e) acquisizione e rinnovo; e
- f) aspetti contrattuali.

▼M2

3 *bis*. L'organo di gestione sviluppa e gestisce un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati contenuti nel CS-SIS. A tale riguardo, esso riferisce periodicamente agli Stati membri.

L'organo di gestione riferisce periodicamente alla Commissione in merito ai problemi incontrati, dandone comunicazione anche agli Stati membri interessati.

La Commissione riferisce periodicamente al Parlamento europeo e al Consiglio in merito ai problemi di qualità dei dati incontrati.

▼B

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

▼ B

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 ⁽¹⁾.

5. Ogni organismo nazionale del settore pubblico di cui al paragrafo 4 soddisfa 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 costruite, capaci, in particolare, di sostenere e garantire il funzionamento continuo di sistemi TI 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. Essa assicura in particolare che la delega non si ripercuota negativamente sull'efficacia dei meccanismi di controllo previsti dal diritto comunitario, siano essi a cura della Corte di giustizia, della Corte dei conti o del garante europeo della protezione dei dati.

▼ M2

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 del presente regolamento, e comprende in particolare le attività di manutenzione e gli adattamenti tecnici necessari per il buon

⁽¹⁾ GU L 248 del 16.9.2002, pag. 1.

▼ M2

funzionamento del sistema. Tali compiti comprendono anche il coordinamento, la gestione e il sostegno delle attività di collaudo per il SIS II centrale e i N.SIS II che garantiscono che il SIS II centrale e i N.SIS II operino secondo i requisiti per la conformità tecnica di cui all'articolo 9.

▼ B*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 45 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);

▼B

- 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 del presente regolamento (autocontrollo).
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 del presente regolamento. 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.

▼M2

3. Se collabora con contraenti esterni per un qualsiasi compito relativo al SIS II, l'organo di gestione monitora da vicino le attività del contraente per garantire il rispetto di tutte le disposizioni del presente regolamento, in particolare sulla sicurezza, la riservatezza e la protezione dei dati.
4. La gestione operativa del CS-SIS non può essere affidata a imprese o organizzazioni private.

▼B*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.

▼B

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 il nome 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 già 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

SEGNALAZIONI DI CITTADINI DI PAESI TERZI AI FINI DEL RIFIUTO DI INGRESSO E DI SOGGIORNO*Articolo 20***Categorie di dati**

1. Fatti salvi l'articolo 8, paragrafo 1 o le disposizioni del presente regolamento 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 nell'articolo 24.

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

▼ B

- 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;

▼ M2

- k *bis*) tipo di reato;

▼ B

- l) azione da intraprendere;
- m) connessioni con altre segnalazioni già introdotte nel SIS II a norma dell'articolo 37.

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 51, paragrafo 2, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.

4. Le norme tecniche necessarie per la consultazione dei dati di cui al paragrafo 2 sono analoghe per le consultazioni nel CS-SIS, nelle copie nazionali e nelle copie tecniche, di cui all'articolo 31, 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.

▼ M2

Qualora la decisione di respingimento e di rifiuto di soggiorno di cui all'articolo 24, paragrafo 2, sia connessa a un reato di terrorismo, il caso è ritenuto adeguato, pertinente e sufficientemente importante da giustificare una segnalazione nel SIS II. Per motivi di sicurezza pubblica o

▼M2

nazionale, gli Stati membri possono eccezionalmente astenersi dall'inserire una segnalazione, quando la stessa rischi di ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari.

*Articolo 22***Norme specifiche per l'inserimento, la verifica o l'interrogazione tramite fotografie e impronte digitali**

1. Fotografie e impronte digitali possono essere inserite solo previo controllo speciale di qualità per accertare che esse soddisfino gli standard minimi di qualità dei dati. Le specifiche sul controllo speciale di qualità sono stabilite secondo la procedura di cui all'articolo 51, paragrafo 2.
2. Qualora siano disponibili dati relativi alle fotografie e alle impronte digitali in una segnalazione nel SIS II, tali dati sono usati per confermare l'identità di una persona reperita grazie all'interrogazione del SIS II con dati alfanumerici.
3. I dati relativi alle impronte digitali possono essere consultati in tutti i casi per identificare una persona. Tuttavia, i dati relativi alle impronte digitali sono consultati per identificare una persona se l'identità della persona non può essere accertata con altri mezzi. A tal fine il SIS II centrale contiene un sistema automatico per il riconoscimento delle impronte digitali (AFIS).
4. I dati relativi alle impronte digitali nel SIS II in relazione a segnalazioni inserite a norma degli articoli 24 e 26 possono essere consultati anche usando serie complete o incomplete di impronte digitali rinvenute sul luogo di un reato grave o di un reato di terrorismo oggetto di indagine, qualora si possa stabilire con un elevato grado di probabilità che tali serie di impronte appartengono a un autore del reato, e purché l'interrogazione sia effettuata simultaneamente nelle pertinenti banche dati nazionali di impronte digitali dello Stato membro.

▼B*Articolo 23***Requisito per inserire una segnalazione**

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

*Articolo 24***Condizioni per la segnalazione ai fini del rifiuto di ingresso o di soggiorno**

1. I dati relativi ai cittadini di paesi terzi per i quali è stata effettuata una segnalazione al fine di rifiutare l'ingresso o il soggiorno sono inseriti sulla base di una segnalazione nazionale risultante da una decisione presa dalle autorità amministrative o giudiziarie competenti conformemente alle norme procedurali stabilite dalla legislazione nazionale, decisione adottata solo sulla base di una valutazione individuale. I ricorsi avverso tali decisioni sono presentati conformemente alla legislazione nazionale.

▼B

2. Una segnalazione è inserita quando la decisione di cui al paragrafo 1 è fondata su una minaccia per l'ordine pubblico, la sicurezza pubblica o la sicurezza nazionale che la presenza del cittadino di un paese terzo in questione può costituire nel territorio di uno Stato membro. Tale situazione si verifica in particolare nei seguenti casi:

- a) se il cittadino di un paese terzo è stato riconosciuto colpevole in uno Stato membro di un reato che comporta una pena detentiva di almeno un anno;
- b) se nei confronti del cittadino di un paese terzo esistono fondati motivi per ritenere che abbia commesso un reato grave o se esistono indizi concreti sull'intenzione di commettere un tale reato nel territorio di uno Stato membro.

3. Una segnalazione può inoltre essere inserita quando la decisione di cui al paragrafo 1 è fondata sul fatto che il cittadino di un paese terzo è stato oggetto di una misura di allontanamento, rifiuto di ingresso o espulsione non revocata né sospesa che comporti o sia accompagnata da un divieto d'ingresso o eventualmente di soggiorno, basata sull'inservanza delle regolamentazioni nazionali in materia di ingresso e di soggiorno dei cittadini di un paese terzo.

4. Il presente articolo non si applica alle persone di cui all'articolo 26.

5. La Commissione riesamina l'applicazione del presente articolo tre anni dopo la data di cui all'articolo 55, paragrafo 2. Alla luce di tale riesame, la Commissione, esercitando il diritto di iniziativa in conformità del trattato, presenta le proposte necessarie per modificare le disposizioni del presente articolo al fine di raggiungere un livello più elevato di armonizzazione dei criteri di inserimento delle segnalazioni.

*Articolo 25***Condizioni per inserire segnalazioni su cittadini di paesi terzi beneficiari del diritto alla libera circolazione all'interno della Comunità**

1. La segnalazione relativa a un cittadino di paese terzo beneficiario del diritto alla libera circolazione all'interno della Comunità ai sensi della direttiva 2004/38/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, relativa al diritto dei cittadini dell'Unione e dei loro familiari di circolare e di soggiornare liberamente nel territorio degli Stati membri⁽¹⁾, è conforme alle norme adottate in esecuzione di tale direttiva.

2. In caso di risposta positiva riguardo a una segnalazione di cui all'articolo 24 su un cittadino di un paese terzo beneficiario del diritto alla libera circolazione all'interno della Comunità, lo Stato membro che effettua la segnalazione consulta immediatamente lo Stato membro che ha effettuato la segnalazione, tramite il suo ufficio SIRENE e in conformità delle disposizioni del manuale SIRENE, al fine di decidere senza indugio l'azione da intraprendere.

⁽¹⁾ GU L 158 del 30.4.2004, pag. 77.

▼ **M2***Articolo 26***Condizioni per inserire la segnalazione di cittadini di paesi terzi oggetto di provvedimenti restrittivi**

1. Le segnalazioni relative a cittadini di paesi terzi oggetto di un provvedimento restrittivo diretto a impedirne l'ingresso o il transito nel territorio degli Stati membri, disposto in conformità di atti giuridici adottati dal Consiglio, compresi i provvedimenti esecutivi di un divieto di viaggio emanato dal Consiglio di sicurezza delle Nazioni Unite, sono inserite nel SIS II, nella misura in cui siano soddisfatte le condizioni relative alla qualità dei dati, ai fini del respingimento e rifiuto di soggiorno.

2. Le segnalazioni sono inserite, aggiornate e cancellate dall'autorità competente dello Stato membro che esercita la presidenza del Consiglio dell'Unione europea al momento dell'adozione della misura. Se detto Stato membro non ha accesso al SIS II o in caso di segnalazioni inserite a norma del presente regolamento, la competenza spetta allo Stato membro che esercita la presidenza successiva e che ha accesso al SIS II, compreso alle segnalazioni inserite a norma del presente regolamento.

Gli Stati membri predispongono le procedure necessarie per inserire, aggiornare e cancellare tali segnalazioni.

▼ **B***Articolo 27***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 dell'accertamento dell'identità dei cittadini di paesi terzi per:

- a) i 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) ⁽¹⁾;
- b) gli altri controlli di polizia e doganali effettuati all'interno dello Stato membro interessato e il 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.

3. Inoltre, il diritto di accesso ai dati inseriti nel SIS II e ai dati riguardanti documenti relativi a persone inseriti a norma dell'articolo 38, paragrafo 2, lettere d) ed e) della ► **C1** decisione 2007/533/GAI ◀ e il

⁽¹⁾ GU L 105 del 13.4.2006, pag. 1.

▼B

diritto di consultare tali dati direttamente può essere esercitato dalle autorità competenti per il rilascio dei visti, dalle autorità centrali competenti per l'esame delle domande di visto e dalle autorità competenti per il rilascio dei permessi di soggiorno e per l'amministrazione della normativa sui cittadini di paesi terzi nel quadro dell'applicazione dell'acquis comunitario in materia di circolazione delle persone. L'accesso ai dati da parte di tali autorità è disciplinato dalla legislazione di ciascuno Stato membro.

4. Le autorità di cui al presente articolo sono inserite nell'elenco di cui all'articolo 31, paragrafo 8.

▼M2*Articolo 27 bis***Accesso di Europol ai dati SIS II**

1. L'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), istituita dal regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ⁽¹⁾, ove necessario all'adempimento del suo mandato, ha il diritto di accedere ai dati nel SIS II e di consultarli. Europol può altresì scambiare e richiedere ulteriori informazioni supplementari in conformità delle disposizioni del manuale SIRENE.

2. Qualora un'interrogazione effettuata da Europol riveli la presenza di una segnalazione nel SIS II, Europol ne informa lo Stato membro segnalante tramite lo scambio di informazioni supplementari a mezzo dell'infrastruttura di comunicazione e conformemente alle disposizioni del manuale SIRENE. Finché non è in grado di utilizzare le funzionalità previste per lo scambio di informazioni supplementari, Europol informa lo Stato membro segnalante tramite i canali definiti dal regolamento (UE) 2016/794.

3. Europol può trattare le informazioni supplementari fornite dagli Stati membri a fini di raffronto con le proprie banche dati e i progetti di analisi operativa, allo scopo di identificare collegamenti o altri nessi pertinenti e per analisi strategiche, tematiche od operative definite all'articolo 18, paragrafo 2, lettere a), b) e c), del regolamento (UE) 2016/794. Qualsiasi trattamento di informazioni supplementari da parte di Europol ai fini del presente articolo è effettuato in conformità di tale regolamento.

4. L'uso da parte di Europol delle informazioni ottenute tramite un'interrogazione del SIS II o tramite il trattamento di informazioni supplementari è soggetto al consenso dello Stato membro segnalante. Se lo Stato membro acconsente all'uso di tali informazioni, il loro trattamento da parte di Europol è disciplinato dal regolamento (UE) 2016/794. Le informazioni sono trasmesse da Europol a paesi terzi e organismi terzi solo con il consenso dello Stato membro segnalante e nel pieno rispetto della normativa dell'Unione in materia di protezione dei dati.

⁽¹⁾ Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 24.5.2016, pag. 53).

▼ M2

5. Europol:

- a) fatti salvi i paragrafi 4 e 6, non collega parti del SIS II, né trasferisce i dati in esso contenuti cui ha accesso, a sistemi di raccolta e trattamento di dati gestito da o presso di essa e non scarica o copia altrimenti parti del SIS II;
- b) in deroga all'articolo 31, paragrafo 1, del regolamento (UE) 2016/794, cancella le informazioni supplementari contenenti dati personali entro un anno dalla cancellazione della relativa segnalazione. A titolo di deroga, se Europol dispone di informazioni nelle proprie banche dati o nei progetti di analisi operativa su un caso cui si riferiscono le informazioni supplementari, Europol può, in via eccezionale, continuare a conservare le informazioni supplementari per svolgere i suoi compiti, ove necessario. Europol informa lo Stato membro segnalante e quello di esecuzione dell'ulteriore conservazione di tali informazioni supplementari e fornisce una giustificazione;
- c) limita l'accesso ai dati nel SIS II, comprese le informazioni supplementari, al proprio personale specificamente autorizzato che necessita dell'accesso a tali dati ai fini dell'assolvimento dei propri compiti;
- d) adotta e applica misure per garantire la sicurezza, la riservatezza e l'autocontrollo a norma degli articoli 10, 11 e 13;
- e) provvede affinché il proprio personale autorizzato a trattare i dati del SIS II riceva una formazione e informazioni adeguate a norma dell'articolo 14;
- f) fatto salvo il regolamento (UE) 2016/794, consente al Garante europeo della protezione dei dati di sorvegliare ed esaminare le attività da essa svolte nell'esercizio del suo diritto di accesso ai dati nel SIS II e di consultazione degli stessi e nello scambio e nel trattamento di informazioni supplementari.

6. Europol può duplicare i dati dal SIS II soltanto per fini tecnici, sempreché tale duplicazione sia necessaria per la consultazione diretta da parte del personale debitamente autorizzato di Europol. Il presente regolamento si applica a tali copie. La copia tecnica è usata soltanto al fine di conservare i dati SIS II mentre tali dati sono consultati. Una volta consultati i dati, la copia è cancellata. Tali usi non sono considerati scaricamento o duplicazione illeciti di dati SIS II. Europol non copia i dati in una segnalazione né i dati complementari trasmessi dagli Stati membri o dal CS-SIS II.

7. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, Europol conserva registri di tutti gli accessi al SIS II e le interrogazioni del SIS II in conformità dell'articolo 12. Tali registri e tale documentazione non sono considerati scaricamenti o duplicazioni illeciti di parti del SIS II.

▼ **M2**

8. Gli Stati membri informano Europol, tramite lo scambio di informazioni supplementari, in merito a qualsiasi riscontro positivo (hit) su segnalazioni relative a reati di terrorismo. Gli Stati membri possono eccezionalmente non informare Europol, se ciò comprometterebbe le indagini in corso, la sicurezza di una persona, o sarebbe in contrasto con gli interessi essenziali della sicurezza dello Stato membro segnalante.

9. Il paragrafo 8 si applica a decorrere dalla data in cui Europol è in grado di ricevere informazioni supplementari in conformità del paragrafo 1.

*Articolo 27 ter***Accesso ai dati nel SIS II da parte delle squadre della guardia di frontiera e costiera europea, di squadre di personale che assolve compiti attinenti al rimpatrio e dei membri delle squadre di sostegno per la gestione della migrazione**

1. A norma dell'articolo 40, paragrafo 8, del regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio ⁽¹⁾, i membri delle squadre di cui all'articolo 2, punti 8) e 9), di tale regolamento hanno, nell'ambito dei rispettivi mandati e a condizione che siano autorizzati a effettuare controlli a norma dell'articolo 27, paragrafo 1, del presente regolamento e abbiano ricevuto la formazione necessaria a norma dell'articolo 14 del presente regolamento il diritto di accedere ai dati nel SIS II e di consultarli, nella misura in cui ciò sia necessario per l'assolvimento dei loro compiti e sia richiesto dal piano operativo per un'operazione specifica. L'accesso ai dati nel SIS II non è esteso ad altri membri delle squadre.

2. I membri delle squadre di cui al paragrafo 1 esercitano il diritto di accedere ai dati nel SIS II e di consultarli in conformità del paragrafo 1 tramite un'interfaccia tecnica. L'interfaccia tecnica è istituita e gestita dall'Agenzia europea della guardia di frontiera e costiera e permette un collegamento diretto con il SIS II centrale.

3. Qualora un'interrogazione effettuata da un membro delle squadre di cui al paragrafo 1 del presente articolo riveli l'esistenza di una segnalazione nel SIS II, lo Stato membro segnalante ne è informato. In conformità dell'articolo 40 del regolamento (UE) 2016/1624, i membri delle squadre intervengono esclusivamente in risposta a una segnalazione nel SIS II sotto il controllo e, di norma, in presenza di guardie di frontiera o di personale che assolve compiti attinenti al rimpatrio dello Stato membro ospitante in cui operano. Lo Stato membro ospitante può autorizzare i membri delle squadre ad agire per suo conto.

4. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, l'Agenzia europea della guardia di frontiera e costiera conserva registri di tutti gli accessi al SIS II e le interrogazioni del SIS II in conformità delle disposizioni dell'articolo 12.

⁽¹⁾ Regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio, del 14 settembre 2016, relativo alla guardia di frontiera e costiera europea che modifica il regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio e che abroga il regolamento (CE) n. 863/2007 del Parlamento europeo e del Consiglio, il regolamento (CE) n. 2007/2004 del Consiglio e la decisione 2005/267/CE del Consiglio (GU L 251 del 16.9.2016, pag. 1).

▼M2

5. L'Agenzia europea della guardia di frontiera e costiera adotta e applica misure per garantire la sicurezza, la riservatezza e l'autocontrollo a norma degli articoli 10, 11 e 13 e provvede affinché le squadre di cui al paragrafo 1 del presente articolo applichino tali misure.

6. Il presente articolo non pregiudica in alcun modo le disposizioni del regolamento (UE) 2016/1624 concernenti la protezione dei dati né la responsabilità dell'Agenzia europea della guardia di frontiera e costiera per trattamenti non autorizzati o scorretti di tali dati.

7. Fatto salvo il paragrafo 2, nessuna parte del SIS II è collegata a un sistema di raccolta e trattamento di dati gestito dalle squadre di cui al paragrafo 1 o dall'Agenzia europea della guardia di frontiera e costiera, e nessun dato nel SIS II a cui hanno accesso tali squadre è trasferito a tale sistema. Nessuna parte del SIS II può essere scaricata o copiata. La registrazione degli accessi e delle interrogazioni non è considerata scaricamento o duplicazione di dati del SIS II.

8. L'Agenzia europea della guardia di frontiera e costiera consente al Garante europeo della protezione dei dati di sorvegliare ed esaminare le attività svolte dalle squadre di cui al presente articolo nell'esercizio del loro diritto di accesso ai dati nel SIS II e di consultazione degli stessi. Ciò non pregiudica le ulteriori disposizioni del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ⁽¹⁾.

▼B*Articolo 28***Ambito dell'accesso**

Gli utenti possono accedere esclusivamente ai dati necessari per l'assolvimento dei loro compiti.

*Articolo 29***Termini di conservazione delle segnalazioni**

1. Le segnalazioni inserite nel SIS II a norma del presente regolamento 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.

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

4. Nel periodo di riesame, lo Stato membro che effettua la segnalazione può decidere, a seguito di una valutazione individuale approfondita, 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.

⁽¹⁾ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

▼B

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 30***Acquisizione di cittadinanza e segnalazioni**

Le segnalazioni relative a persone che hanno acquisito la cittadinanza di uno Stato i cui cittadini sono beneficiari del diritto alla libera circolazione all'interno della Comunità sono cancellate non appena lo Stato membro che ha effettuato la segnalazione viene a conoscenza o viene informato a norma dell'articolo 34 di tale acquisizione.

CAPO V

REGOLE GENERALI SUL TRATTAMENTO DEI DATI*Articolo 31***Trattamento dei dati SIS II**

1. Gli Stati membri possono trattare i dati di cui all'articolo 20 ai fini del rifiuto di ingresso o di soggiorno nei loro territori.

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 27. Le disposizioni del presente regolamento 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 per un periodo non superiore a quarantotto ore. Tale periodo può essere esteso in caso di emergenza, finché l'emergenza non sia cessata.

Fatto salvo il primo comma, le copie tecniche che portano alla creazione di banche dati off-line ad uso delle autorità preposte al rilascio dei visti non sono più permesse un anno dopo che l'autorità in questione è stata collegata con successo all'infrastruttura di comunicazione per il sistema d'informazione da prevedere in un futuro regolamento concernente il sistema d'informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata fatta eccezione per le copie destinate ad essere usate esclusivamente in caso di emergenza in seguito all'indisponibilità della rete per oltre 24 ore.

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

▼B

4. L'accesso ai dati è autorizzato esclusivamente nei limiti delle competenze delle autorità nazionali di cui all'articolo 27 e riservato al personale debitamente autorizzato.

5. I dati non possono essere usati a scopi amministrativi. A titolo di deroga, i dati inseriti a norma del presente regolamento possono essere usati conformemente alle legislazioni di ciascuno Stato membro dalle autorità di cui all'articolo 27, paragrafo 3 nell'assolvimento dei loro doveri.

6. I dati inseriti a norma dell'articolo 24 del presente regolamento e i dati relativi a documenti concernenti persone inseriti a norma dell'articolo 38, paragrafo 2, lettere d) ed e) della ►**C1** decisione 2007/533/GAI ◀ possono essere usati conformemente alle legislazioni nazionali di ciascun Stato membro ai fini indicati all'articolo 27, paragrafo 3 del presente regolamento.

7. Qualsiasi uso dei dati non conforme ai paragrafi da 1 a 6 è considerato un uso illegale ai sensi della legislazione nazionale 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 del presente regolamento 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 comunitario non preveda disposizioni particolari, la legislazione di ciascuno Stato membro è applicabile ai dati inseriti nel rispettivo N. SIS II.

*Articolo 32***Dati SIS II e archivi nazionali**

1. L'articolo 31, 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 31, 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 33***Informazione in caso di mancata segnalazione**

Se un'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 34

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 36.

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 dello scambio di informazioni supplementari.

Articolo 35

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 riguardi o meno la stessa persona;

▼B

- 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 34, 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 36***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 soltanto 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) data e luogo di nascita;
- d) sesso;
- e) fotografie;
- f) impronte digitali;
- g) cittadinanza(e);
- h) numero del o dei documenti d'identità e data del rilascio.

▼B

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 51, paragrafo 2, 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 37***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 nel presente regolamento. Le autorità che non hanno diritto di accedere 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 51, paragrafo 2, fatte salve le disposizioni dello strumento che istituisce l'organo di gestione.



Articolo 38

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 39

Trasferimento di dati personali a terzi

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

CAPO VI

PROTEZIONE DEI DATI

Articolo 40

Trattamento di categorie di dati sensibili

È vietato il trattamento delle categorie di dati di cui all'articolo 8, paragrafo 1 della direttiva 95/46/CE.

Articolo 41

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 al presente regolamento è esercitato nel rispetto della legislazione dello Stato membro presso il quale l'interessato lo fa valere.

▼B

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 42***Diritto di informazione**

1. I cittadini di paesi terzi oggetto di una segnalazione a norma del presente regolamento sono informati a norma degli articoli 10 e 11 della direttiva 95/46/CE. Le informazioni sono fornite per iscritto insieme a una copia della decisione nazionale che ha dato origine alla segnalazione o a un riferimento a detta decisione di cui all'articolo 24, paragrafo 1.
2. Le informazioni non sono fornite:
 - a) qualora:
 - i) i dati personali non siano stati raccolti presso il cittadino di un paese terzo interessato;
 - e
 - ii) la fornitura dell'informazione si riveli impossibile o richieda sforzi sproporzionati;
 - b) qualora il cittadino di un paese terzo interessato sia già informato;

▼B

- c) laddove la legislazione nazionale consenta che il diritto di informazione sia limitato, in particolare per salvaguardare la sicurezza nazionale, la difesa, la pubblica sicurezza e la prevenzione, la ricerca, l'accertamento e il perseguimento di reati.

*Articolo 43***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 48.

▼C1

3. La Commissione valuta le norme sui mezzi di impugnazione di cui al presente articolo entro il 17 gennaio 2009.

▼B*Articolo 44***Controllo di N. SIS II**

1. L'autorità o le autorità designate in ciascuno Stato membro che dispongono dei poteri di cui all'articolo 28 della direttiva 95/46/CE («autorità nazionale di controllo») controllano 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 nazionale di controllo disponga delle risorse sufficienti per assolvere i compiti ad essa assegnati a norma del presente regolamento.

*Articolo 45***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 in conformità del presente regolamento. Si applicano di conseguenza i

▼B

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 46***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 del presente regolamento, 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 47***Protezione dei dati durante il periodo transitorio**

La Commissione, qualora durante il periodo transitorio deleghi le sue competenze a 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 VII
RESPONSABILITÀ E SANZIONI

Articolo 48

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 contro 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 il presente regolamento.
3. Se l'inosservanza da parte di uno Stato membro degli obblighi derivanti dal presente regolamento 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 partecipante al SIS II non abbiano ommesso di adottare le misure ragionevolmente necessarie a evitare tali danni o a minimizzarne gli effetti.

Articolo 49

Sanzioni

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

CAPO VIII
DISPOSIZIONI FINALI

Articolo 50

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

▼B

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 del presente regolamento con riguardo al SIS II centrale, la sicurezza del SIS II centrale e le eventuali implicazioni per 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.

8. Durante un periodo transitorio, prima che l'organo di gestione assuma le sue responsabilità, la Commissione è responsabile della presentazione e della trasmissione delle relazioni di cui ai paragrafi 3 e 4.

*Articolo 51***Comitato**

1. La Commissione è assistita da un comitato.
2. Nei casi in cui è fatto riferimento al presente paragrafo, si applicano gli articoli 5 e 7 della decisione 1999/468/CE, tenendo conto delle disposizioni dell'articolo 8 della stessa.

Il termine di cui all'articolo 5, paragrafo 6 della decisione 1999/468/CE è fissato a tre mesi.

3. Il comitato esercita la sua funzione a partire dalla data di entrata in vigore del presente regolamento.

*Articolo 52***Modifica delle disposizioni dell'acquis di Schengen**

1. Per le materie che rientrano nell'ambito di applicazione del trattato, il presente regolamento sostituisce, alla data di cui all'articolo 55, paragrafo 2, le disposizioni degli articoli da 92 a 119 della convenzione di Schengen, salvo l'articolo 102 bis.

▼B

2. Esso sostituisce anche, alla data di cui all'articolo 55, paragrafo 2, le seguenti disposizioni dell'acquis di Schengen che attuano quegli articoli ⁽¹⁾:

- 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 28 aprile 1999 riguardante i costi d'installazione del C. SIS (SCH/Com-ex (99) 4);
- f) Decisione del Comitato esecutivo del 28 aprile 1999 riguardante l'aggiornamento del Manuale SIRENE (SCH/Com-ex (99) 5);
- g) Dichiarazione del Comitato esecutivo del 18 aprile 1996 relativa alla definizione del concetto di straniero (SCH/Com-ex (96) decl. 5);
- h) Dichiarazione del Comitato esecutivo del 28 aprile 1999 riguardante la struttura del SIS (SCH/Com-ex (99) decl. 2 riv.);
- i) 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, i riferimenti agli articoli della convenzione di Schengen così sostituiti e alle pertinenti disposizioni dell'acquis di Schengen che li attuano si intendono fatti al presente regolamento.

*Articolo 53***Abrogazione**

Alla data di cui all'articolo 55, paragrafo 2, sono abrogati i regolamenti (CE) n. 378/2004 e (CE) n. 871/2004 e le decisioni 2005/451/GAI, 2005/728/GAI e 2006/628/CE.

⁽¹⁾ GU L 239 del 22.9.2000, pag. 439.



Articolo 54

Periodo transitorio e bilancio

1. Le segnalazioni sono trasferite dal SIS 1 + al SIS II. Gli Stati membri assicurano, attribuendo priorità alle segnalazioni di persone, che il contenuto delle segnalazioni trasferite dal SIS 1+ al SIS II sia conforme alle disposizioni del presente regolamento prima possibile e al più tardi entro tre anni dalla data di cui all'articolo 55, paragrafo 2. Nel periodo transitorio gli Stati membri possono continuare ad applicare gli articoli 94 e 96 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 del presente regolamento 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 del presente regolamento, senza tuttavia ritardare l'azione da intraprendere in base alla stessa.

2. Alla data fissata a norma dell'articolo 55, paragrafo 2 il residuo del bilancio approvato in conformità alle 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 alla 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, nel presente regolamento, all'organo di gestione si intendono fatti alla Commissione.

Articolo 55

Entrata in vigore, applicabilità e migrazione

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

2. Esso 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+.

▼B

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 preso 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*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri in conformità del trattato che istituisce la Comunità europea.