UNIONE EUROPEA

IL PARLAMENTO EUROPEO **IL CONSIGLIO**

Bruxelles, 28 novembre 2018
(OR. en)

2016/0408 (COD)
LEX 1848

PE-CONS 35/1/18
REV 1

SIRIS 70
FRONT 189
SCHENGEN 29
COMIX 334
CODEC 1125

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO SULL'ISTITUZIONE, L'ESERCIZIO E L'USO DEL SISTEMA D'INFORMAZIONE SCHENGEN (SIS) NEL SETTORE DELLE VERIFICHE DI FRONTIERA, CHE MODIFICA LA CONVENZIONE DI APPLICAZIONE DELL'ACCORDO DI SCHENGEN E ABROGA IL REGOLAMENTO (CE) N. 1987/2006

REGOLAMENTO (UE) 2018/...
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 28 novembre 2018

sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 77, paragrafo 2, lettere b) e d), e l'articolo 79, paragrafo 2, lettera c),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria[1],

[1] Posizione del Parlamento europeo del 24 ottobre 2018 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 19 novembre 2018.

considerando quanto segue:

(1) Il sistema d'informazione Schengen (SIS) rappresenta uno strumento fondamentale per l'applicazione delle disposizioni dell'*acquis* di Schengen integrate nell'ambito dell'Unione europea. Il SIS è una delle principali misure compensative che contribuiscono a mantenere un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, sostenendo la cooperazione operativa tra le autorità nazionali competenti, in particolare guardie di frontiera, autorità di polizia e doganali, autorità competenti per l'immigrazione, autorità competenti a fini di prevenzione, accertamento, indagine o perseguimento di reati o esecuzione di sanzioni penali.

(2) Inizialmente il SIS è stato 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[1], firmata il 19 giugno 1990 (convenzione di applicazione dell'accordo di Schengen). L'incarico di sviluppare il SIS di seconda generazione (SIS II) è stato affidato alla Commissione in virtù del regolamento (CE) n. 2424/2001 del Consiglio[2] e della decisione 2001/886/GAI del Consiglio[3]. Il SIS II è stato successivamente istituito con regolamento (CE) n. 1987/2006[4] del Parlamento europeo e del Consiglio e con la decisione 2007/533/GAI del Consiglio[5]. Il SIS II ha sostituito il SIS istituito sulla base della convenzione di applicazione dell'accordo di Schengen.

---

1 GU L 239 del 22.9.2000, pag. 19.

2 Regolamento (CE) n. 2424/2001 del Consiglio, del 6 dicembre 2001, sullo sviluppo del Sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 328 del 13.12.2001, pag. 4).

3 Decisione 2001/886/GAI del Consiglio, del 6 dicembre 2001, sullo sviluppo del Sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 328 del 13.12.2001, pag. 1).

4 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).

5 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) (GU L 205 del 7.8.2007, pag. 63).

(3) Tre anni dopo l'entrata in funzione del SIS II, la Commissione ha svolto una valutazione del sistema ai sensi del regolamento (CE) n. 1987/2006 e della decisione 2007/533/GAI. Il 21 dicembre 2016 la Commissione ha presentato la relazione di valutazione del SIS di seconda generazione (SIS II) ai sensi dell'articolo 24, paragrafo 5, dell'articolo 43, paragrafo 3, e dell'articolo 50, paragrafo 5 del regolamento (CE) n. 1987/2006, e dell'articolo 59, paragrafo 3, e dell'articolo 66, paragrafo 5 della decisione 2007/533/GAI nonché il relativo documento di lavoro dei servizi al Parlamento europeo e al Consiglio. Le raccomandazioni espresse in tali documenti dovrebbero essere recepite, se del caso, nel presente regolamento.

(4) Il presente regolamento costituisce la base giuridica per il SIS nelle materie rientranti nell'ambito di applicazione della parte terza, titolo V, capo 2, del trattato sul funzionamento dell'Unione europea (TFUE). Il regolamento (UE) 2018/... del Parlamento europeo e del Consiglio[1+] costituisce la base giuridica per il SIS nelle materie rientranti nell'ambito di applicazione del titolo V, capi 4 e 5della parte terza del TFUE.

---

[1] Regolamento (UE) 2018/… del Parlamento europeo e del Consiglio del ... sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica ed abroga la decisione 2007/533/GAI del Consiglio e abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L ...).

[+] GU: inserire il numero di serie nel testo e completare nella nota in calce il riferimento di pubblicazione del regolamento di cui al doc. PE-CONS 36/18.

(5) Il fatto che la base giuridica per il SIS consti di strumenti distinti non pregiudica il principio secondo il quale il SIS costituisce un unico sistema d'informazione che dovrebbe operare in quanto tale. Esso dovrebbe includere un'unica rete di uffici nazionali denominati uffici SIRENE al fine di garantire lo scambio di informazioni supplementari. È pertanto opportuno che alcune disposizioni di tali strumenti siano identiche.

(6) È necessario specificare gli obiettivi del SIS, alcuni elementi della sua architettura tecnica e del suo finanziamento, fissare regole relative al suo esercizio e uso da un'estremità all'altra e definire le competenze. È altresì necessario determinare le categorie di dati da inserire nel sistema, le finalità dell'inserimento e del trattamento dei dati e i relativi criteri. Sono altresì necessarie norme concernenti la cancellazione delle segnalazioni, le autorità abilitate ad accedere ai dati, l'uso di dati biometrici, nonché norme che specifichino ulteriormente gli obblighi sulla protezione e sul trattamento dei dati.

(7) Le segnalazioni nel SIS contengono solo le informazioni necessarie per identificare una persona e l'azione da intraprendere. Gli Stati membri dovrebbero quindi, all'occorrenza, scambiare informazioni supplementari relative alle segnalazioni.

(8) Il SIS consta di un sistema centrale (SIS centrale) e di sistemi nazionali. I sistemi nazionali potrebbero contenere una copia completa o parziale della banca dati del SIS che può essere condivisa da due o più Stati membri. Poiché il SIS è il più importante strumento di scambio di informazioni in Europa volto a garantire la sicurezza e la gestione efficace delle frontiere, è necessario garantirne il funzionamento ininterrotto a livello sia centrale sia nazionale. La disponibilità del SIS dovrebbe essere soggetta a un attento monitoraggio a livello centrale e degli Stati membri e ogni incidente che implichi un'indisponibilità per gli utenti finali dovrebbe essere registrato e comunicato ai portatori di interesse a livello nazionale e dell'Unione. Ogni Stato membro dovrebbe creare una copia di riserva (backup) per il proprio sistema nazionale. Gli Stati membri dovrebbero inoltre garantire una connettività senza interruzioni al SIS centrale con punti di connessione duplicati e separati fisicamente e geograficamente. Il SIS centrale e l'infrastruttura di comunicazione dovrebbero essere gestiti in modo da assicurarne il loro funzionamento 24 ore su 24 e 7 giorni su 7. Per questo motivo, l'agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia ("eu-LISA"), istituita dal regolamento (UE) 2018/... del Parlamento europeo e del Consiglio[1+] dovrebbe mettere in atto soluzioni tecniche volte a rafforzare la disponibilità ininterrotta del SIS, fatte salve una valutazione d'impatto indipendente e un'analisi costi-benefici.

---

[1] Regolamento (UE) 2018/... del Parlamento europeo e del Consiglio, del ..., relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), che modifica il regolamento (CE) n. 1987/2006 e la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (UE) n. 1077/2011 (GU L ...).

[+] GU: inserire il numero di serie nel testo e completare nella nota in calce il riferimento di pubblicazione del regolamento di cui al doc. PE-CONS 29/18.

(9) È necessario tenere un manuale aggiornato recante le modalità dettagliate di scambio di informazioni supplementari relative alle azioni da intraprendere in seguito alle segnalazioni ("manuale SIRENE"). Gli uffici SIRENE dovrebbero garantire lo scambio di tali informazioni in modo rapido ed efficace.

(10) Per provvedere a uno scambio efficace di informazioni supplementari, anche riguardo alle specifiche azioni da intraprendere in seguito alle segnalazioni, è opportuno potenziare il funzionamento degli uffici SIRENE introducendo requisiti sulle risorse disponibili, sulla formazione degli utenti e sui termini di risposta alle richieste ricevute da altri uffici SIRENE.

(11) Gli Stati membri dovrebbero assicurare che il personale del proprio ufficio SIRENE possieda le competenze linguistiche e la conoscenza del diritto e delle norme procedurali pertinenti che sono necessari allo svolgimento dei suoi compiti.

(12) Per poter beneficiare pienamente delle funzionalità del SIS, gli Stati membri dovrebbero provvedere affinché gli utenti finali e il personale degli uffici SIRENE ricevano periodicamente una formazione, anche in materia di sicurezza e protezione dei dati nonché di qualità dei dati. Gli uffici SIRENE dovrebbero essere coinvolti nell'elaborazione dei programmi di formazione. Per quanto possibile, gli uffici SIRENE dovrebbero inoltre prevedere scambi di personale con altri uffici SIRENE almeno una volta all'anno. Gli Stati membri sono incoraggiati ad adottare misure adeguate per evitare che la rotazione del personale comporti perdite di competenze e di esperienza.

(13) La gestione operativa delle componenti centrali del SIS è esercitata dall'eu-LISA. Per consentire all'eu-LISA di dedicare le risorse finanziarie e umane necessarie a coprire tutti gli aspetti della gestione operativa del SIS centrale e dell'infrastruttura di comunicazione, il presente regolamento dovrebbe stabilirne dettagliatamente i compiti, in particolare riguardo agli aspetti tecnici dello scambio di informazioni supplementari.

(14) Fatti salvi la responsabilità degli Stati membri riguardo all'esattezza dei dati inseriti nel SIS e al ruolo degli uffici SIRENE quali coordinatori della qualità, l'eu-LISA dovrebbe assumere la competenza di migliorare la qualità dei dati introducendo uno strumento di monitoraggio centrale della qualità dei dati e dovrebbe presentare a intervalli regolari relazioni alla Commissione e agli Stati membri. La Commissione dovrebbe riferire al Parlamento europeo e al Consiglio sui problemi di qualità dei dati riscontrati. Per migliorare ulteriormente la qualità dei dati inseriti nel SIS, l'eu-LISA dovrebbe inoltre offrire una formazione sull'uso del SIS agli organismi nazionali di formazione e, nella misura del possibile, agli uffici SIRENE e agli utenti finali.

(15) Per consentire di monitorare meglio l'uso del SIS e per analizzare le tendenze relative alla pressione migratoria e alla gestione delle frontiere, l'eu-LISA dovrebbe essere in grado di sviluppare una capacità avanzata di fornire statistiche agli Stati membri, al Parlamento europeo, al Consiglio, alla Commissione, a Europol e all'Agenzia europea della guardia di frontiera e costiera, senza compromettere l'integrità dei dati. È opportuno pertanto istituire un archivio centrale. Nessuna delle statistiche contenute nell'archivio o prodotte dallo stesso dovrebbe contenere dati personali. Nell'ambito della cooperazione tra autorità di controllo e il garante europeo della protezione dei dati ai sensi del presente regolamento, gli Stati membri dovrebbero comunicare statistiche relative all'esercizio del diritto di accesso, rettifica di dati inesatti e cancellazione di dati archiviati illecitamente.

(16) È opportuno introdurre nuove categorie di dati nel SIS per consentire agli utenti finali di adottare decisioni informate sulla base di una segnalazione senza perdere tempo. Pertanto, le segnalazioni ai fini del respingimento e del rifiuto di soggiorno dovrebbero comprendere informazioni sulla decisione su cui si basa la segnalazione. Inoltre, per facilitare l'identificazione delle persone e individuare i casi di identità molteplici, la segnalazione dovrebbe includere, se tale informazione fosse disponibile, un riferimento al documento d'identificazione personale della persona interessata o al numero di identificazione personale e una copia, possibilmente a colori, di tale documento.

(17) Le autorità competenti dovrebbero avere la possibilità, se strettamente necessario, di inserire nel SIS informazioni specifiche relative a qualsiasi caratteristica fisica particolare, oggettiva e inalterabile di una persona, quali tatuaggi, cicatrici o altri segni.

(18) Laddove disponibili, tutti i dati pertinenti, in particolare il nome della persona interessata, dovrebbero essere inseriti in fase di creazione di una segnalazione, per ridurre al minimo il rischio di falsi riscontri positivi (hit) e attività operative non necessarie.

(19) Il SIS non dovrebbe conservare i dati usati per l'interrogazione, ad eccezione dei registri conservati per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati, per l'autocontrollo e per garantire il corretto funzionamento dei sistemi nazionali, l'integrità e la sicurezza dei dati.

(20) Per contribuire alla corretta identificazione degli interessati, il SIS dovrebbe consentire il trattamento di dati biometrici. Qualsiasi inserimento nel SIS di fotografie, immagini del volto o dati dattiloscopici, cosi come qualsiasi utilizzo di tali dati, dovrebbe essere limitato a quanto necessario ai fini degli obiettivi perseguiti, dovrebbe essere autorizzato dal diritto dell'Unione, dovrebbe avvenire nel rispetto dei diritti fondamentali, in particolare dell'interesse superiore del minore, e dovrebbe essere conforme alla normativa dell'Unione in materia di protezione dei dati, ivi comprese le pertinenti disposizioni sulla protezione dei dati previste dal presente regolamento. Nella stessa ottica, per evitare i disagi causati da errori di identificazione, il SIS dovrebbe inoltre consentire il trattamento di dati relativi a persone la cui identità è stata usurpata (), fatti salvi adeguate garanzie, l'ottenimento del consenso dell'interessato per ciascuna categoria di dati, in particolare per le impronte palmari, e la rigorosa limitazione delle finalità per cui tali dati personali possono essere lecitamente trattati.

(21) Gli Stati membri dovrebbero adottare le disposizioni tecniche necessarie affinché gli utenti finali, ogni volta che sono autorizzati a consultare una banca dati della polizia nazionale o dell'immigrazione, consultino parallelamente anche il SIS nel rispetto dei principi di cui all'articolo 4 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio[1] e all'articolo 5 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[2]. Ciò dovrebbe permettere al SIS di funzionare come principale misura compensativa nello spazio senza controlli alle frontiere interne e di contrastare meglio la dimensione transfrontaliera della criminalità e la mobilità dei criminali.

(22) È opportuno che il presente regolamento stabilisca le condizioni per l'uso dei dati dattiloscopici, delle fotografie e delle immagini del volto a fini di identificazione e di verifica. L'uso di immagini del volto e di fotografie a fini di identificazione dovrebbe inizialmente aver luogo solo presso i valichi di frontiera regolari. Tale uso dovrebbe essere sottoposto a una relazione della Commissione che confermi che la tecnologia necessaria è disponibile, affidabile e pronta ad essere usata.

---

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

2 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

(23) È opportuno permettere di consultare dati dattiloscopici conservati nel SIS con serie complete o incomplete di impronte digitali o impronte palmari rilevate sul luogo di un reato se si può stabilire con un grado molto elevato di probabilità che appartengono all'autore di un reato grave o di un reato di terrorismo e purché un'interrogazione sia effettuata simultaneamente nelle pertinenti banche dati nazionali di impronte digitali. È opportuno rivolgere un'attenzione particolare alla definizione di norme di qualità applicabili alla conservazione dei dati biometrici.

(24) Allorché l'identità di una persona non possa essere accertata con altri mezzi, si dovrebbero utilizzare i dati dattiloscopici per l'identificazione. Dovrebbe essere consentito in tutti i casi identificare una persona utilizzando dati dattiloscopici.

(25) Gli Stati membri dovrebbero avere la possibilità di stabilire connessioni fra le segnalazioni nel SIS. La creazione di connessioni fra due o più segnalazioni non dovrebbe incidere sull'azione da eseguire, né sui termini di riesame della segnalazione o sui diritti di accesso alle segnalazioni.

(26) È possibile migliorare il grado di efficacia, armonizzazione e coerenza sancendo l'obbligo di inserire nel SIS tutti i divieti d'ingresso emessi dalle autorità nazionali competenti secondo procedure conformi alla direttiva 2008/115/CE del Parlamento europeo e del Consiglio[1] e stabilendo norme comuni sull'inserimento di segnalazioni ai fini del respingimento o del rifiuto di soggiorno in seguito al rimpatrio del cittadino di paese terzo il cui soggiorno è irregolare. Gli Stati membri dovrebbero adottare tutte le misure necessarie per garantire che non intercorra alcun lasso di tempo fra il momento in cui il cittadino di paese terzo interessato lascia lo spazio Schengen e l'attivazione della segnalazione nel SIS. Si dovrebbe così garantire l'esecuzione dei divieti d'ingresso ai valichi di frontiera esterni, impedendo di fatto il rientro nello spazio Schengen.

(27) Le persone nei cui confronti sia stata emessa una decisione di respingimento o di rifiuto di soggiorno dovrebbero avere il diritto di proporre ricorso avverso tale decisione. Il diritto di ricorso dovrebbe essere conforme alla direttiva 2008/115/CE nel caso della decisione in materia di rimpatrio.

---

1 Direttiva 2008/115/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, recante norme e procedure comuni applicabili negli Stati membri al rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 348 del 24.12.2008, pag. 98).

(28) È opportuno che il presente regolamento stabilisca norme obbligatorie sulla consultazione delle autorità nazionali, e sulla comunicazione alle stesse, nei casi in cui uno Stato membro intenda effettuare o abbia già effettuato una segnalazione ai fini del respingimento o del rifiuto di soggiorno di un cittadino di paese terzo che tuttavia è titolare di un permesso di soggiorno o di un visto per soggiorno di lunga durata validi, rilasciati da un altro Stato membro, ovvero possa ottenerli. Si tratta di situazioni che generano grandi incertezze per le guardie di frontiera, le forze di polizia e le autorità competenti per l'immigrazione. Per garantire che i cittadini di paesi terzi aventi il diritto di risiedere legalmente nel territorio degli Stati membri possano entrare in tale territorio senza difficoltà ed escludere da tale possibilità chi non gode del diritto di entrarvi, è pertanto opportuno fissare termini obbligatori per una consultazione rapida e concludente.

(29) Quando si cancella una segnalazione nel SIS in seguito a una consultazione tra Stati membri, lo Stato membro segnalante dovrebbe poter mantenere il cittadino di paese terzo in questione nel proprio elenco nazionale delle persone segnalate.

(30) Il presente regolamento non dovrebbe pregiudicare l'applicazione della direttiva 2004/38/CE del Parlamento europeo e del Consiglio[1].

[1] 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, che modifica il regolamento (CEE) n. 1612/68 ed abroga le direttive 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE (GU L 158 del 30.4.2004, pag. 77).

(31) Le segnalazioni non dovrebbero essere conservate nel SIS oltre il periodo necessario per la realizzazione delle finalità specifiche per le quali sono state inserite. Entro tre anni dal suo inserimento nel SIS, lo Stato membro segnalante dovrebbe riesaminare la necessità di conservare una segnalazione. Tuttavia, se la decisione nazionale su cui si basa la segnalazione prevede un periodo di validità superiore a tre anni, la segnalazione dovrebbe essere riesaminata entro cinque anni. La decisione di mantenere le segnalazioni di persone dovrebbe essere basata su una valutazione individuale approfondita. Gli Stati membri dovrebbero esaminare le segnalazioni di persone entro il periodo di riesame prescritto e dovrebbero tenere statistiche sul numero di segnalazioni di persone per le quali il periodo di conservazione è stato prolungato.

(32) L'inserimento di una segnalazione nel SISS e la proroga della data di scadenza di una segnalazione nel SIS dovrebbero essere soggetti a un requisito obbligatorio di proporzionalità, in base al quale si verifichi se l'adeguatezza, la pertinenza e l'importanza del caso giustifichino l'inserimento della segnalazione nel SIS. Nell'ipotesi di reati di terrorismo, il caso dovrebbe essere ritenuto adeguato, pertinente e sufficientemente importante da giustificare l'esistenza di una segnalazione nel SIS. Per motivi di sicurezza pubblica o nazionale, gli Stati membri dovrebbero poter eccezionalmente astenersi dall'inserire una segnalazione nel SIS qualora la stessa rischi di ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari.

(33) L'integrità dei dati SIS è di primaria importanza. È opportuno pertanto stabilire garanzie adeguate per il trattamento dei dati SIS a livello sia centrale sia nazionale, per garantire la sicurezza dei dati da un'estremità all'altra. Le autorità competenti per il trattamento dei dati dovrebbero essere vincolate ai requisiti di sicurezza previsti dal presente regolamento e dovrebbero essere soggette a una procedura uniforme di segnalazione degli incidenti. Il loro personale dovrebbe essere adeguatamente formato e informato di eventuali reati e sanzioni al riguardo.

(34) I dati trattati nel SIS e le relative informazioni supplementari scambiate a norma del presente regolamento non dovrebbero essere trasferiti a paesi terzi o ad organizzazioni internazionali, né essere messi a loro disposizione.

(35) Per rafforzare l'efficacia del lavoro delle autorità competenti per l'immigrazione nel decidere in merito al diritto di un cittadino di paese terzo di entrare e soggiornare nel territorio degli Stati membri, così come in merito al rimpatrio di un cittadino di paese terzo il cui soggiorno è irregolare, è opportuno concedere a dette autorità l'accesso al SIS a norma del presente regolamento.

(36) Fatte salve le norme più specifiche di cui al presente regolamento concernenti il trattamento dei dati personali, al trattamento dei dati personali da parte degli Stati membri ai sensi del presente regolamento si dovrebbe applicare il regolamento (UE) 2016/679, a meno che tale trattamento sia effettuato dalle autorità competenti nazionali a fini di prevenzione, indagine, accertamento o perseguimento di reati di terrorismo o di altri reati gravi.

(37) Fatte salve le norme più specifiche di cui al presente regolamento, al trattamento dei dati personali da parte delle autorità competenti nazionali a fini di prevenzione, accertamento, indagine o perseguimento di reati di terrorismo o di altri reati gravi o esecuzione di sanzioni penali ai sensi del presente regolamento si dovrebbero applicare le disposizioni legislative, regolamentari e amministrative nazionali adottate a norma della direttiva (UE) 2016/680. L'accesso ai dati inseriti nel SIS e il diritto di consultazione degli stessi da parte delle autorità nazionali competenti a fini di prevenzione, accertamento, indagine o perseguimento di reati di terrorismo o di altri reati gravi o esecuzione di sanzioni penali sono subordinati a tutte le pertinenti disposizioni del presente regolamento e a quelle della direttiva (UE) 2016/680 recepite nel diritto interno, e in particolare alla sorveglianza delle autorità di controllo di cui alla direttiva (UE) 2016/680.

(38) Il regolamento (UE) 2018/...[+] del Parlamento europeo e del Consiglio[1] dovrebbe applicarsi al trattamento dei dati personali effettuato dalle istituzioni e dagli organismi dell'Unione nell'assolvimento dei loro compiti a norma del presente regolamento.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 31/18.

[1] Regolamento (UE) 2018/… del Parlamento europeo e del Consiglio, del ..., concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L …).

(39) Il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio[1] dovrebbe applicarsi al trattamento dei dati personali effettuato da Europol a norma del presente regolamento.

(40) Quando utilizzano il SIS, le autorità competenti dovrebbero assicurare il rispetto della dignità e dell'integrità della persona i cui dati sono trattati. Il trattamento di dati personali ai fini del presente regolamento non deve dar luogo a discriminazioni nei confronti delle persone fondate sul sesso, sulla razza o sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale.

(41) Nella misura in cui riguardano la riservatezza, le pertinenti disposizioni dello statuto dei funzionari e del regime applicabile agli altri agenti dell'Unione europea stabilito dal Regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio[2] ("statuto dei funzionari") dovrebbero applicarsi ai funzionari o altri agenti che sono impiegati e che lavorano per il SIS.

(42) Sia gli Stati membri sia l'eu-LISA dovrebbero mantenere piani 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.

---

[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).

[2] GU L 56 del 4.3.1968, pag. 1.

(43) Le autorità nazionali di controllo indipendenti di cui al regolamento (UE) 2016/679 e alla direttiva (UE) 2016/680 ("autorità di controllo") dovrebbero controllare la liceità del trattamento dei dati personali da parte degli Stati membri ai sensi del presente regolamento, incluso lo scambio di informazioni supplementari. Le autorità di controllo dovrebbe essere dotata di risorse sufficienti per svolgere detto compito. È opportuno stabilire i diritti degli interessati in materia di accesso, rettifica e cancellazione dei dati personali che li riguardano conservati nel SIS e i conseguenti diritti di ricorso dinanzi ai giudici nazionali, nonché il reciproco riconoscimento delle sentenze. È inoltre opportuno esigere dagli Stati membri statistiche annuali.

(44) Le autorità di controllo dovrebbero provvedere affinché sia svolto un controllo delle operazioni di trattamento dei dati nei sistemi nazionali dei rispettivi Stati membri, conformemente alle norme di revisione internazionali, almeno ogni quattro anni. Il controllo dovrebbe essere svolto dalle autorità di controllo oppure le autorità di controllo dovrebbero commissionare il controllo direttamente a un revisore indipendente nel settore della protezione dei dati. Il revisore indipendente dovrebbe rimanere sotto il controllo e la responsabilità delle autorità di controllo interessate, che di conseguenza dovrebbero commissionare esse stesse la revisione, definirne chiaramente la finalità, l'ambito di applicazione e la metodologia, fornire istruzioni e supervisionare il controllo e i relativi risultati finali.

(45) Il Garante europeo della protezione dei dati dovrebbe controllare le attività delle istituzioni e degli organismi dell'Unione relative al trattamento dei dati personali a norma del presente regolamento. Il Garante europeo della protezione dei dati e le autorità di controllo dovrebbero cooperare nel controllo del SIS.

(46) Al Garante europeo della protezione dei dati dovrebbero essere fornite risorse sufficienti per assolvere i compiti assegnatigli a norma del presente regolamento, compresa l'assistenza da parte di persone competenti in materia di dati biometrici.

(47) A norma del regolamento (UE) 2016/794, Europol sostiene e potenzia l'azione delle autorità competenti nazionali e la loro cooperazione nel combattere il terrorismo e altre forme gravi di criminalità e fornisce analisi e valutazioni della minaccia. Per facilitare ad Europol l'esecuzione dei suoi compiti, in particolare nell'ambito del Centro europeo contro il traffico di migranti, è opportuno accordare ad Europol l'accesso alle categorie di segnalazioni stabilite nel presente regolamento.

(48) Per colmare le lacune nella condivisione di informazioni sul terrorismo, in particolare sui combattenti terroristi stranieri - di cui è cruciale sorvegliare i movimenti - gli Stati membri sono incoraggiati a condividere con Europol informazioni su attività legate al terrorismo. È opportuno che tale condivisione di informazioni sia effettuata mediante lo scambio di informazioni supplementari con Europol sulle segnalazioni pertinenti. A tale scopo Europol dovrebbe istituire una connessione con l'infrastruttura di comunicazione.

(49) È inoltre necessario stabilire regole chiare a uso di Europol sul trattamento e sullo scaricamento dei dati SIS per consentire ad Europol di usare SIS in modo ampio, purché siano rispettate le norme in materia di protezione dei dati previste dal presente regolamento e dal regolamento (UE) 2016/794. Qualora le interrogazioni svolte da Europol nel SIS rivelino l'esistenza di una segnalazione inserita da uno Stato membro, Europol non può intraprendere l'azione richiesta. Dovrebbe pertanto informare lo Stato membro interessato tramite lo scambio di informazioni supplementari con il rispettivo ufficio SIRENE per consentire allo Stato membro di dare seguito al caso.

(50) Il regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio[1] prevede, ai fini di tale regolamento, che lo Stato membro ospitante autorizzi i membri delle squadre di cui all'articolo 2, punto 8), di tale regolamento dispiegate dall'Agenzia europea della guardia di frontiera e costiera a consultare le banche dati nell'Unione se tale consultazione è necessaria a conseguire gli obiettivi operativi specificati nel piano operativo per i controlli di frontiera, la sorveglianza di frontiera e i rimpatri. Altre agenzie competenti dell'Unione, in particolare l'Ufficio europeo di sostegno per l'asilo ed Europol, possono altresì distaccare presso le squadre di sostegno per la gestione della migrazione esperti che non fanno parte del personale di tali agenzie dell'Unione. L'impiego delle squadre di cui all'articolo 2, punti 8) e 9), di tale regolamento ha l'obiettivo di offrire un rinforzo operativo e tecnico agli Stati membri richiedenti, in particolare a quelli che devono affrontare sfide migratorie sproporzionate. Per assolvere i compiti loro assegnati, le squadre di cui all'articolo 2, punti 8) e 9), di tale regolamento hanno bisogno di accedere al SIS tramite un'interfaccia tecnica dell'Agenzia europea della guardia di frontiera e costiera connessa al SIS centrale. Qualora le interrogazioni svolte nel SIS dalla squadra di cui all'articolo 2, punti 8) e 9) del regolamento (UE) 2016/1624 o dalle squadre del personale rivelino l'esistenza di una segnalazione inserita da uno Stato membro, il membro della squadra o del personale non può intraprendere l'azione richiesta se non è autorizzato a farlo dallo Stato membro ospitante. Pertanto lo Stato membro ospitante dovrebbe essere informato al fine di dare seguito al caso. Lo Stato membro ospitante dovrebbe comunicare il riscontro positivo (hit) allo Stato membro segnalante tramite lo scambio di informazioni supplementari.

---

[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).

(51) Taluni aspetti del SIS non possono essere trattati con esaustività dal presente regolamento a causa della loro natura tecnica, del loro dettaglio e della necessità di aggiornamenti periodici. Tali aspetti includono, ad esempio, le norme tecniche concernenti l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati, la qualità dei dati, le regole relative ai dati biometrici, le norme sulla compatibilità e sull'ordine delle priorità delle segnalazioni, l'interconnessione delle segnalazioni e lo scambio di informazioni supplementari. È pertanto opportuno attribuire 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.

(52) È opportuno attribuire alla Commissione competenze di esecuzione al fine di garantire condizioni uniformi di esecuzione del presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[1]. La procedura di adozione degli atti di esecuzione a norma del presente regolamento e del regolamento (UE) 2018/...[+] dovrebbe essere la stessa.

(53) Per ragioni di trasparenza è opportuno che due anni dopo l'entrata in funzione del SIS a norma del presente regolamento, l'eu-LISA presenti una relazione sul funzionamento tecnico del SIS centrale e dell'infrastruttura di comunicazione, compresa la relativa sicurezza, e sullo scambio bilaterale e multilaterale di informazioni supplementari. Ogni quattro anni la Commissione dovrebbe provvedere a una valutazione globale.

---

[1] Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

[+] GU: inserire il numero di serie del regolamento di cui al PE-CONS 36/18.

(54) Al fine di garantire il corretto funzionamento del SIS, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE per quanto riguarda la determinazione dei casi in cui è possibile ricorrere a fotografie e immagini del volto per identificare le persone in un contesto diverso da quello dei valichi di frontiera regolari. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[1]. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(55) Poiché gli obiettivi del presente regolamento, vale a dire l'istituzione e la regolamentazione di un sistema d'informazione dell'Unione e il relativo scambio di informazioni supplementari, non possono essere conseguiti in misura sufficiente dagli Stati membri, ma, a motivo della loro stessa natura, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

[1] GU L 123 del 12.5.2016, pag. 1.

(56) Il presente regolamento rispetta i diritti fondamentali e osserva i principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea. In particolare, il presente regolamento rispetta pienamente la tutela dei dati personali in conformità dell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea prefiggendosi nel contempo l'obiettivo di garantire un ambiente sicuro per tutte le persone residenti sul territorio dell'Unione e di difendere i migranti irregolari dallo sfruttamento e dalla tratta di esseri umani. Nei casi relativi ai minori l'interesse superiore del minore dovrebbe costituire una considerazione preminente.

(57) I costi stimati dell'aggiornamento dei sistemi nazionali e dell'applicazione delle nuove funzionalità previste dal presente regolamento sono inferiori all'importo rimanente nella linea di bilancio per le "Frontiere intelligenti" ricompresa nel regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio[1]. Di conseguenza, è opportuno che il finanziamento destinato allo sviluppo di sistemi informatici a sostegno della gestione dei flussi migratori attraverso le frontiere esterne a norma del regolamento (UE) n. 515/2014 venga assegnato agli Stati membri e all'eu-LISA. È opportuno monitorare i costi finanziari dell'aggiornamento del SIS nonché l'attuazione del presente regolamento. In caso di costi stimati più elevati è opportuno che siano messi a disposizione finanziamenti dell'Unione per sostenere gli Stati membri conformemente al quadro finanziario pluriennale applicabile.

[1] Regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, che istituisce, nell'ambito del Fondo sicurezza interna, lo strumento di sostegno finanziario per le frontiere esterne e i visti e che abroga la decisione n. 574/2007/CE (GU L 150 del 20.5.2014, pag. 143).

(58) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al TUE e al TFUE, la Danimarca non partecipa all'adozione del presente regolamento, non è da esso vincolata, né è soggetta alla sua applicazione. Dato che il presente regolamento si basa sull'*acquis* di Schengen, la Danimarca decide, ai sensi dell'articolo 4 di tale protocollo, entro un periodo di sei mesi dalla decisione del Consiglio sul presente regolamento, se intende recepirlo nel proprio diritto interno.

(59) Il presente regolamento costituisce uno sviluppo delle disposizioni dell'*acquis* di Schengen a cui il Regno Unito non partecipa, a norma della decisione 2000/365/CE del Consiglio[1]; il Regno Unito non partecipa pertanto alla sua adozione, non è da esso vincolato né è soggetto alla sua applicazione.

(60) Il presente regolamento costituisce uno sviluppo delle disposizioni dell'*acquis* di Schengen a cui l'Irlanda non partecipa, a norma della decisione 2002/192/CE del Consiglio[2]; l'Irlanda non partecipa pertanto alla sua adozione, non è da esso vincolata né è soggetta alla sua applicazione.

---

1 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 disposizioni dell'*acquis* di Schengen (GU L 131 dell'1.6.2000, pag. 43).

2 Decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'*acquis* di Schengen (GU L 64 del 7.3.2002, pag. 20).

(61) Per quanto riguarda l'Islanda e la Norvegia, il presente regolamento costituisce, 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[1], uno sviluppo delle disposizioni dell'*acquis* di Schengen che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE del Consiglio[2].

(62) Per quanto riguarda la Svizzera, il presente regolamento costituisce, ai sensi dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen[3], uno sviluppo delle disposizioni dell'*acquis* di Schengen che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE del Consiglio, in combinato disposto con l'articolo 3 della decisione 2008/146/CE del Consiglio[4].

---

1 GU L 176 del 10.7.1999, pag. 36.

2 Decisione 1999/437/CE del Consiglio, del 17 maggio 1999, relativa a talune modalità di applicazione dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sull'associazione di questi due Stati all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen (GU L 176 del 10.7.1999, pag. 31).

3 GU L 53 del 27.2.2008, pag. 52.

4 Decisione 2008/146/CE del Consiglio, del 28 gennaio 2008, relativa alla conclusione, a nome della Comunità europea, 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 53 del 27.2.2008, pag. 1).

(63) Per quanto riguarda il Liechtenstein, il presente regolamento costituisce, ai sensi del protocollo tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'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[1], uno sviluppo delle disposizioni dell'*acquis* di Schengen che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE del Consiglio, in combinato disposto con l'articolo 3 della decisione 2011/350/UE del Consiglio[2].

(64) Per quanto riguarda Bulgaria e Romania, il presente regolamento costituisce un atto basato sull'*acquis* di Schengen o a esso altrimenti connesso ai sensi dell'articolo 4, paragrafo 2, dell'atto di adesione del 2005, e dovrebbe essere letto in combinato disposto con la decisione 2010/365/UE del Consiglio[3] e la decisione (UE) 2018/934 del Consiglio[4].

---

1 GU L 160 del 18.6.2011, pag. 21.

2 Decisione 2011/350/UE del Consiglio, del 7 marzo 2011, sulla conclusione, a nome dell'Unione europea, del protocollo tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'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, con particolare riguardo alla soppressione dei controlli alle frontiere interne e alla circolazione delle persone (GU L 160 del 18.6.2011, pag. 19).

3 Decisione 2010/365/UE del Consiglio, del 29 giugno 2010, sull'applicazione delle disposizioni dell'*acquis* di Schengen relative al sistema d'informazione Schengen nella Repubblica di Bulgaria e in Romania (GU L 166 dell'1.7.2010, pag. 17).

4 Decisione (UE) 2018/934 del Consiglio, del 25 giugno 2018, relativa all'attuazione delle rimanenti disposizioni dell'*acquis* di Schengen concernenti il sistema d'informazione Schengen nella Repubblica di Bulgaria e in Romania (GU L 165 del 2.7.2018, pag. 37).

(65) Per quanto riguarda la Croazia, il presente regolamento costituisce un atto basato sull'*acquis* di Schengen o a esso altrimenti connesso ai sensi dell'articolo 4, paragrafo 2, dell'atto di adesione del 2011, e dovrebbe essere letto in combinato disposto con la decisione (UE) 2017/733 del Consiglio[1].

(66) Per quanto riguarda Cipro, il presente regolamento costituisce un atto basato sull'*acquis* di Schengen o a esso altrimenti connesso ai sensi dell'articolo 3, paragrafo 2, dell'atto di adesione del 2003.

(67) Il presente regolamento introduce una serie di miglioramenti al SIS che accresceranno la sua efficacia, rafforzeranno la protezione dei dati ed estenderanno i diritti di accesso. Alcuni di questi miglioramenti non richiedono sviluppi tecnici complessi, mentre altri richiedono modifiche tecniche di varia entità. Affinché i miglioramenti del sistema possano essere messi a disposizione degli utenti finali il più rapidamente possibile, il presente regolamento introduce modifiche al regolamento (CE) n. 1987/2006 in diverse tappe. Vari miglioramenti al sistema dovrebbero applicarsi immediatamente al momento dell'entrata in vigore del presente regolamento, mentre altri dovrebbero applicarsi uno o due anni dopo la sua entrata in vigore. Il presente regolamento dovrebbe applicarsi in tutti i suoi elementi entro tre anni dalla sua entrata in vigore. Al fine di evitare ritardi nella sua applicazione, l'attuazione per tappe del presente regolamento dovrebbe essere oggetto di attento monitoraggio.

---

[1] Decisione (UE) 2017/733 del Consiglio, del 25 aprile 2017, sull'applicazione delle disposizioni dell'*acquis* di Schengen relative al sistema d'informazione Schengen nella Repubblica di Croazia (GU L 108 del 26.4.2017, pag. 31).

(68) Il regolamento (CE) n. 1987/2006 dovrebbe essere abrogato con effetto a decorrere dalla data di piena applicazione del presente regolamento.

(68) Il Garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio[1] e ha espresso un parere il 3 maggio 2017,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

[1] 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 (GU L 8 del 12.1.2001, pag. 1).

Capo I
Disposizioni generali

Articolo 1

Scopo generale del SIS

Scopo del SIS è assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, inclusi il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri, e garantire l'applicazione delle disposizioni della parte terza, titolo V, capo 2, del TFUE relative alla circolazione delle persone in detto territorio, avvalendosi delle informazioni trasmesse mediante tale sistema.

Articolo 2

Oggetto

1. Il presente regolamento stabilisce le condizioni e le procedure applicabili all'inserimento e al trattamento nel SIS delle segnalazioni riguardanti cittadini di paesi terzi e allo scambio di informazioni supplementari e dati complementari ai fini del respingimento e del rifiuto di soggiorno nel territorio degli Stati membri.

2. Il presente regolamento contempla anche disposizioni sull'architettura tecnica del SIS, sulle competenze degli Stati membri e dell'agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia ("eu-LISA"), sulle regole sul trattamento dei dati, sui diritti delle persone interessate e sulla responsabilità.

Articolo 3

Definizioni

Ai fini del presente regolamento s'intende per:

1) "segnalazione": un insieme di dati inseriti nel SIS che permette alle autorità competenti di identificare una persona al fine di intraprendere un'azione specifica;

2) "informazioni supplementari": le informazioni non facenti parte dei dati di segnalazione conservati nel SIS ma connesse alle segnalazioni inserite nel SIS, che devono essere scambiate tramite gli uffici SIRENE:

   a) per permettere agli Stati membri di consultarsi o informarsi a vicenda quando introducono una segnalazione;

   b) in seguito a un riscontro positivo (hit) al fine di consentire l'azione appropriata;

   c) quando non è possibile procedere all'azione richiesta;

d) con riguardo alla qualità dei dati SIS;

e) con riguardo alla compatibilità e alla priorità delle segnalazioni;

f) con riguardo ai diritti di accesso;

3) "dati complementari": i dati memorizzati nel SIS e connessi alle segnalazioni inserite nel SIS, che devono essere immediatamente disponibili per le autorità competenti nei casi in cui una persona i cui dati sono stati inseriti nel SIS sia localizzata grazie all'interrogazione del SIS;

4) "cittadino di paese terzo": chi non è cittadino dell'Unione ai sensi dell'articolo 20, paragrafo 1, TFUE, a eccezione di chi, in virtù di accordi conclusi tra l'Unione, o tra l'Unione e i suoi Stati membri, da un lato, e paesi terzi, dall'altro, beneficia di diritti in materia di libera circolazione equivalenti a quelli dei cittadini dell'Unione;

5) "dati personali": dati personali quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679;

6) "trattamento dei dati personali": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la memorizzazione, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

7) "corrispondenza": il verificarsi, nell'ordine, di quanto segue:

a) un utente finale ha effettuato un'interrogazione;

b) l'interrogazione ha rivelato la presenza di una segnalazione inserita nel SIS da un altro Stato membro; e

c) i dati relativi alla segnalazione nel SIS corrispondono ai dati dell'interrogazione;

8) "riscontro positivo (hit)": una corrispondenza che soddisfi i seguenti criteri:

a) è stata confermata da:

i) l'utente finale; oppure,

ii) l'autorità competente conformemente alle procedure nazionali qualora la corrispondenza in questione sia basata sul raffronto di dati biometrici;

e

b) sono richieste ulteriori azioni;

9) "Stato membro segnalante": lo Stato membro che ha inserito la segnalazione nel SIS;

10) "Stato membro di rilascio": lo Stato membro che esamina la possibilità di rilasciare o di prorogare un permesso di soggiorno o un visto per soggiorno di lunga durata o che lo ha rilasciato o prorogato, ed è coinvolto nella procedura di consultazione con un altro Stato membro;

11) "Stato membro di esecuzione": lo Stato membro che intraprende o ha intrapreso l'azione richiesta in seguito a un riscontro positivo (hit);

12) "utente finale": membro del personale di un'autorità competente autorizzato ad interrogare direttamente il CS-SIS, l'N.SIS o una loro copia tecnica;

13) "dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche o fisiologiche di una persona fisica che ne consentono o confermano l'identificazione univoca, vale a dire fotografie, immagini del volto e dati dattiloscopici;

14) "dati dattiloscopici": dati relativi alle impronte digitali e alle impronte palmari che, per il loro carattere di unicità e i punti caratteristici che contengono, permettono confronti precisi e irrefutabili sull'identità di una persona;

15) "immagine del volto": le immagini digitali del volto caratterizzate da sufficiente risoluzione e qualità dell'immagine per essere utilizzate in un raffronto biometrico automatizzato;

16) "rimpatrio": il rimpatrio quale definito nell'articolo 3, punto 3), della direttiva 2008/115/CE;

17) "divieto d'ingresso": il divieto d'ingresso quale definito nell'articolo 3, punto 6), della direttiva 2008/115/CE;

18) "reati di terrorismo": i reati previsti dal diritto nazionale di cui agli articoli da 3 a 14 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio[1] o equivalenti a uno di tali reati per gli Stati membri che non sono vincolati da detta direttiva;

19) "permesso di soggiorno": il permesso di soggiorno quale definito nell'articolo 2, punto 16), del regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio[2];

20) "visto per soggiorno di lunga durata": il visto per soggiorno di lunga durata di cui all'articolo 18, paragrafo 1, della convenzione d'applicazione dell'accordo di Schengen;

21) "minaccia per la salute pubblica": minaccia per la salute pubblica quale definita nell'articolo 2, punto 21), regolamento (UE) 2016/399.

Articolo 4

Architettura tecnica e modalità operative del SIS

1. Il SIS consta di:

a) un sistema centrale ("SIS centrale") costituito da:

i) un'unità di supporto tecnico ("CS-SIS") che contiene una banca dati, la "banca dati del SIS", e che include un CS-SIS di riserva,

---

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

2 Regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio, del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen) (GU L 77 del 23.3.2016, pag. 1).

ii) un'interfaccia nazionale uniforme ("NI-SIS");

b) un sistema nazionale ("N.SIS") in ciascuno Stato membro, composto dei sistemi di dati nazionali che comunicano con il SIS centrale, e che includa almeno un N.SIS di riserva (backup site) nazionale o condiviso; e

c) un'infrastruttura di comunicazione fra il CS-SIS, il CS-SIS di riserva e l'NI-SIS ("infrastruttura di comunicazione") che fornisce una rete virtuale cifrata dedicata ai dati SIS e provvede allo scambio di informazioni tra gli uffici SIRENE ai sensi dell'articolo 7, paragrafo 2.

Un N.SIS di cui alla lettera b) può contenere un archivio di dati ("copia nazionale"), contenente a sua volta una copia completa o parziale della banca dati del SIS. Due o più Stati membri possono creare una copia condivisa in uno dei loro N.SIS, che può essere usata congiuntamente dagli Stati membri in questione. Tale copia condivisa è considerata la copia nazionale di ciascuno di tali Stati membri.

Un N.SIS di riserva condiviso di cui alla lettera b) può essere usato congiuntamente da due o più Stati membri. In tal caso, l'N.SIS di riserva è considerato l'N.SIS di riserva di ciascuno di tali Stati membri. L'N.SIS e la sua copia di riserva possono essere usati simultaneamente per garantire agli utenti finali una disponibilità ininterrotta.

Gli Stati membri che intendono creare una copia condivisa o un N.SIS di riserva condiviso da utilizzare congiuntamente definiscono le rispettive responsabilità in un accordo scritto. Essi notificano il proprio accordo alla Commissione.

L'infrastruttura di comunicazione sostiene e contribuisce a garantire la disponibilità ininterrotta del SIS. Essa comprende percorsi ridondanti e separati per le connessioni tra il CS-SIS e il CS-SIS di riserva, oltre che percorsi ridondanti e separati per le connessioni tra ciascun punto di accesso nazionale alla rete SIS e il CS-SIS e il CS-SIS di riserva.

2. Gli Stati membri inseriscono, aggiornano, cancellano e consultano i dati SIS attraverso il proprio N.SIS. Gli Stati membri che utilizzano una copia nazionale parziale o completa, o una copia condivisa parziale o completa rendono disponibile tale copia ai fini dell'interrogazione automatizzata nel territorio di ciascuno di tali Stati membri. La copia nazionale o condivisa parziale contiene almeno i dati di cui all'articolo 20, paragrafo 2, lettere da a) a v). Non possono essere consultati gli archivi di dati contenuti nell'N.SIS degli altri Stati membri, salvo in caso di copie condivise.

3. Il CS-SIS svolge funzioni di controllo tecnico e di gestione e dispone di una copia di riserva del CS-SIS in grado di assicurare tutte le funzionalità del CS-SIS principale in caso di guasto. Il CS-SIS e il CS-SIS di riserva sono ubicati nei due siti tecnici dell'eu-LISA.

4. L'eu-LISA mette in atto soluzioni tecniche volte a rafforzare la disponibilità ininterrotta del SIS o mediante il funzionamento simultaneo del CS-SIS e il CS-SIS di riserva, purché il CS-SIS di riserva sia in grado di assicurare il funzionamento del SIS in caso di guasto del CS-SIS, o mediante la duplicazione del sistema o delle sue componenti. In deroga ai requisiti procedurali di cui all'articolo 10 del regolamento (UE) 2018/...[+] l'eu-LISA elabora, al più tardi ... [un anno dopo l'entrata in vigore del presente regolamento], uno studio sulle opzioni per le soluzioni tecniche, contenente una valutazione d'impatto indipendente e un'analisi costi-benefici.

5. In circostanze eccezionali, l'eu-LISA può, se necessario, creare temporaneamente una copia supplementare della banca dati del SIS.

6. Il CS-SIS fornisce i servizi necessari per l'inserimento e il trattamento dei dati SIS, compresa la consultazione della banca dati del SIS. Per gli Stati membri che usano una copia nazionale o condivisa, il CS-SIS provvede a quanto segue:

   a) aggiornamento in linea delle copie nazionali;

   b) sincronizzazione e coerenza tra le copie nazionali e la banca dati del SIS; e

   c) funzioni di inizializzazione e ripristino delle copie nazionali.

7. Il CS-SIS assicura una disponibilità ininterrotta.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 29/18.

Articolo 5

Costi

1. I costi relativi all'esercizio, alla manutenzione e all'ulteriore sviluppo del SIS centrale e dell'infrastruttura di comunicazione sono a carico del bilancio generale dell'Unione. Tali costi includono il lavoro effettuato con riguardo al CS-SIS per garantire la fornitura dei servizi di cui all'articolo 4, paragrafo 6.

2. È assegnato un finanziamento tratto dalla dotazione di 791 milioni di EUR prevista all'articolo 5, paragrafo 5, lettera b), del regolamento (UE) n. 515/2014 per coprire i costi di attuazione del presente regolamento.

3. Dalla dotazione di cui al paragrafo 2, e fatti salvi ulteriori finanziamenti a tal fine provenienti da altre fonti del bilancio generale dell'Unione, è assegnato all'eu-LISA un importo di 31 098 000 EUR. Tale finanziamento è attuato mediante gestione indiretta e contribuisce alla realizzazione degli sviluppi tecnici richiesti in virtù del presente regolamento con riguardo al SIS centrale e all'infrastruttura di comunicazione, nonché alle correlate attività di formazione.

4. Dalla dotazione di cui al paragrafo 2 gli Stati membri partecipanti al regolamento (UE) n. 515/2014 ricevono una dotazione globale supplementare pari a 36 810 000 EUR da ripartire in parti uguali tramite una somma forfettaria in aggiunta alla loro dotazione di base. Tale finanziamento è attuato in regime di gestione concorrente ed è destinato interamente all'aggiornamento rapido ed efficace dei sistemi nazionali rilevanti in linea con i requisiti del presente regolamento.

5. I costi per l'istituzione, l'esercizio, la manutenzione e l'ulteriore sviluppo di ciascun N.SIS 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, la manutenzione e l'ulteriore sviluppo del proprio N.SIS e per il collegamento all'NI-SIS.

Ciascuno Stato membro è responsabile di garantire la disponibilità ininterrotta dei dati SIS agli utenti finali.

Ciascuno Stato membro trasmette le proprie segnalazioni tramite il proprio N.SIS.

Articolo 7

Ufficio N.SIS e ufficio SIRENE

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

   Tale autorità è responsabile del corretto funzionamento e della sicurezza dell'N.SIS, garantisce l'accesso delle autorità competenti al SIS e adotta le misure atte a garantire l'osservanza del presente regolamento. Ha il compito di garantire che tutte le funzionalità del SIS siano messe adeguatamente a disposizione degli utenti finali.

2. Ciascuno Stato membro designa un'autorità nazionale, operativa 24 ore su 24 e 7 giorni su 7, che garantisca lo scambio e la disponibilità di tutte le informazioni supplementari ("ufficio SIRENE") conformemente al manuale SIRENE. Ogni ufficio SIRENE funge da punto di contatto unico per il proprio Stato membro per lo scambio di informazioni supplementari sulle segnalazioni e per agevolare l'adozione delle azioni richieste quando sono inserite nel SIS segnalazioni relative a persone e tali persone sono reperite in seguito a un riscontro positivo (hit).

   Ogni ufficio SIRENE dispone, in conformità della legislazione nazionale, di un facile accesso diretto o indiretto a tutte le informazioni nazionali pertinenti, comprese le banche dati nazionali e tutte le informazioni sulle segnalazioni degli Stati Membri, nonché alla consulenza di esperti per essere in grado di reagire alle richieste di informazioni supplementari in modo rapido ed entro i termini di cui all'articolo 8.

Gli uffici SIRENE coordinano la verifica della qualità delle informazioni inserite nel SIS. A tal fine, essi hanno accesso ai dati trattati nel SIS.

3. Gli Stati membri forniscono all'eu-LISA gli estremi dei rispettivi uffici N. SIS e SIRENE. L'eu-LISA pubblica l'elenco degli uffici N. SIS e SIRENE insieme all'elenco di cui all'articolo 41, paragrafo 8.

Articolo 8

Scambio di informazioni supplementari

1. Le informazioni supplementari sono scambiate conformemente alle disposizioni del manuale SIRENE e tramite l'infrastruttura di comunicazione. Gli Stati membri forniscono le risorse tecniche e umane necessarie per garantire in permanenza la disponibilità e lo scambio tempestivo ed efficace delle informazioni supplementari. In caso di indisponibilità dell'infrastruttura di comunicazione, gli Stati membri usano altri mezzi tecnici adeguatamente protetti per lo scambio di informazioni supplementari. Un elenco di mezzi tecnici adeguatamente protetti è riportato nel manuale SIRENE.

2. Le informazioni supplementari sono usate solo per le finalità per le quali sono state trasmesse in conformità dell'articolo 49, a meno che non sia stato ottenuto il previo consenso per un uso ulteriore dallo Stato membro segnalante.

3. Gli uffici SIRENE svolgono i loro compiti in modo rapido ed efficiente, in particolare rispondendo a una richiesta di informazioni supplementari appena possibile e comunque entro 12 ore dal ricevimento della richiesta.

Le richieste di informazioni supplementari da trattare con la massima priorità possono recare la dicitura "URGENT" (urgente) nei formulari SIRENE, seguita dalla specificazione dei motivi dell'urgenza.

4. La Commissione adotta atti di esecuzione al fine di stabilire norme dettagliate per i compiti degli uffici SIRENE ai sensi del presente regolamento e per lo scambio di informazioni supplementari sotto forma di un manuale intitolato "manuale SIRENE". Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

Articolo 9

Conformità tecnica e funzionale

1. Per consentire una pronta ed efficiente trasmissione dei dati, all'atto dell'istituzione del rispettivo N.SIS ciascuno Stato membro si conforma alle norme, ai protocolli e alle procedure tecniche comuni stabiliti per assicurare la compatibilità del proprio N.SIS con il SIS Centrale.

2. In caso di uso di una copia nazionale, lo Stato membro interessato assicura, tramite i servizi forniti dal CS-SIS e gli aggiornamenti automatici di cui all'articolo 4, paragrafo 6, che i dati memorizzati nella copia nazionale siano identici e coerenti con quelli della banca dati del SIS e che un'interrogazione nella copia nazionale produca risultati equivalenti a quelli di un'interrogazione effettuata nella banca dati del SIS.

3. Gli utenti finali ricevono i dati necessari allo svolgimento dei loro compiti, in particolare, e se necessario, tutti i dati disponibili che consentano di identificare l'interessato e di intraprendere le azioni necessarie.

4. Gli Stati membri e l'eu-LISA effettuano prove regolari per verificare la conformità tecnica delle copie nazionali di cui al paragrafo 2. I risultati di tali prove sono presi in considerazione nel quadro del meccanismo istituito dal regolamento (UE) n. 1053/2013 del Consiglio[1].

5. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme, i protocolli e le procedure tecniche comuni di cui al paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

[1] Regolamento (UE) n. 1053/2013 del Consiglio, del 7 ottobre 2013, che istituisce un meccanismo di valutazione e di controllo per verificare l'applicazione dell'*acquis* di Schengen e che abroga la decisione del comitato esecutivo del 16 settembre 1998 che istituisce una Commissione permanente di valutazione e di applicazione di Schengen (GU L 295 del 6.11.2013, pag. 27).

Articolo 10

Sicurezza – Stati membri

1. Ciascuno Stato membro, in relazione al proprio N.SIS, adotta le misure necessarie, compresi un piano di sicurezza, un piano di continuità operativa e un piano di ripristino in caso di disastro al fine di:

   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 dei dati personali (controllo all'ingresso delle installazioni);

   c) impedire che i supporti di dati siano letti, copiati, modificati o rimossi 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 sistemi automatizzati di trattamento dei dati mediante apparecchiature per la trasmissione di dati (controllo degli utenti);

   f) impedire che i dati siano trattati nel SIS senza autorizzazione e che i dati trattati nel SIS siano modificati o cancellati senza autorizzazione (controllo dell'inserimento dei dati);

g) garantire che le persone autorizzate a usare un sistema automatizzato di trattamento dei dati possano accedere solo ai dati previsti dalla loro autorizzazione di accesso attraverso identificatori di utente individuali e unici ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);

h) assicurare che tutte le autorità con diritto di accesso al SIS o alle installazioni di trattamento dei 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 di controllo di cui all'articolo 55, paragrafo 1, a richiesta di queste (profili del personale);

i) garantire la possibilità di verificare e accertare a quali organismi possano essere trasmessi dati personali mediante apparecchiature per la trasmissione di dati (controllo della trasmissione);

j) garantire la possibilità di verificare e accertare a posteriori quali dati personali siano stati introdotti nei sistemi automatizzati di trattamento dei dati, il momento dell'inserimento, la persona che lo ha effettuato e la finalità dello stesso (controllo dell'inserimento);

k) 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);

l) monitorare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure organizzative relative al monitoraggio interno per garantire l'osservanza del presente regolamento (autocontrollo);

m) garantire che, in caso di interruzione, i sistemi installati possano essere ripristinati (ripristino); e

n) garantire che il SIS esegua le sue funzioni correttamente, che gli errori siano segnalati (affidabilità) e che i dati personali conservati nel SIS non possano essere falsati da un errore di funzionamento del sistema (integrità).

2. Gli Stati membri adottano misure equivalenti a quelle del paragrafo 1 per quanto riguarda la sicurezza del trattamento e degli scambi di informazioni supplementari, fra l'altro garantendo la sicurezza dei locali degli uffici SIRENE.

3. Gli Stati membri adottano misure equivalenti a quelle del paragrafo 1 del presente articolo per quanto riguarda la sicurezza del trattamento dei dati SIS da parte delle autorità di cui all'articolo 34.

4. Le misure descritte nei paragrafi 1, 2 e 3 possono rientrare in un approccio alla sicurezza e in un piano di sicurezza generici a livello nazionale comprendenti molteplici sistemi informatici. In tali casi, i requisiti di cui al presente articolo e la relativa applicabilità al SIS sono chiaramente identificabili in tale piano e garantiti dallo stesso.

Articolo 11

Riservatezza – Stati membri

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

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

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

Articolo 12

Tenuta dei registri a livello nazionale

1. Gli Stati membri provvedono affinché ogni accesso ai dati personali e ogni scambio dei medesimi nell'ambito del CS-SIS siano registrati nei rispettivi N.SIS per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati, ai fini dell'autocontrollo e per garantire il corretto funzionamento dell'N.SIS, nonché l'integrità e la sicurezza dei dati. Tale requisito non si applica ai processi automatici di cui all'articolo 4, paragrafo 6, lettere a), b) e c).

2. I registri riportano, in particolare, la cronistoria della segnalazione, la data e l'ora dell'attività di trattamento dei dati, i dati usati per effettuare un'interrogazione, un riferimento ai dati trattati e gli identificatori di utente individuali e unici dell'autorità competente e della persona che effettua il trattamento dei dati.

3. In deroga al paragrafo 2 del presente articolo, se l'interrogazione è effettuata con dati dattiloscopici o un'immagine del volto in conformità dell'articolo 33, i registri riportano il tipo di dati usati per effettuare l'interrogazione anziché i dati effettivi.

4. I registri sono utilizzati solo ai fini di cui al paragrafo 1 e sono cancellati tre anni dopo la loro creazione. I registri contenenti la cronistoria delle segnalazioni sono cancellati tre anni dopo la cancellazione delle segnalazioni.

5. I registri possono essere tenuti più a lungo dei termini di cui al paragrafo 4 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, ai fini dell'autocontrollo e per garantire il corretto funzionamento dell'N.SIS e 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 compiti.

Articolo 13

Autocontrollo

Gli Stati membri provvedono affinché ogni autorità con diritto di accesso ai dati SIS adotti le misure necessarie per conformarsi al presente regolamento e cooperi, se necessario, con l'autorità di controllo.

Articolo 14

Formazione del personale

1. Prima di essere autorizzato a trattare dati conservati nel SIS e periodicamente dopo che è stato accordato l'accesso ai dati SIS, il personale delle autorità con diritto di accesso al SIS riceve una formazione adeguata sulla sicurezza dei dati, sui diritti fondamentali, comprese le norme sulla protezione dei dati, nonché sulle procedure di trattamento dei dati previste nel manuale SIRENE. Il personale è informato delle disposizioni relative ai reati e alle sanzioni pertinenti, comprese quelle stabilite all'articolo 59.

2. Gli Stati membri dispongono di un programma nazionale di formazione sul SIS che comprende una formazione per gli utenti finali e per il personale degli uffici SIRENE.

   Tale programma di formazione può rientrare in un programma di formazione generale a livello nazionale comprendente la formazione in altri settori pertinenti.

3. Almeno una volta l'anno sono organizzati corsi comuni di formazione a livello dell'Unione per rafforzare la cooperazione tra gli uffici SIRENE.

Capo III
Competenze dell'eu-LISA

Articolo 15

Gestione operativa

1. L'eu-LISA è responsabile della gestione operativa del SIS centrale. L'eu-LISA, in collaborazione con gli Stati membri, provvede affinché per il SIS centrale siano utilizzate in ogni momento le migliori tecnologie disponibili, fatta salva un'analisi costi-benefici.

2. L'eu-LISA è inoltre responsabile dei seguenti compiti relativi all'infrastruttura di comunicazione:

   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.

3. L'eu-LISA è inoltre responsabile dei seguenti compiti relativi agli uffici SIRENE e alla comunicazione tra gli uffici SIRENE:

a) coordinamento, gestione e sostegno delle attività di collaudo;

b) gestione e aggiornamento di specifiche tecniche per lo scambio di informazioni supplementari tra gli uffici SIRENE e l'infrastruttura di comunicazione; e

c) gestione dell'effetto dei cambiamenti tecnici laddove riguardino sia il SIS che lo scambio di informazioni supplementari tra gli uffici SIRENE.

4. L'eu-LISA sviluppa e gestisce un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati contenuti nel CS-SIS. A tale riguardo essa riferisce periodicamente agli Stati membri.

L'eu-LISA riferisce periodicamente alla Commissione in merito ai problemi incontrati e agli Stati membri interessati.

La Commissione presenta una relazione periodica al Parlamento europeo e al Consiglio in merito ai problemi di qualità dei dati riscontrati.

5. L'eu-LISA svolge anche compiti relativi all'offerta di formazione sull'uso tecnico del SIS e sulle misure atte a migliorare la qualità dei dati SIS.

6. La gestione operativa del SIS centrale consiste nell'insieme dei compiti necessari al funzionamento 24 ore su 24 e 7 giorni su 7 del SIS centrale in conformità del presente regolamento, e comprende in particolare le attività di manutenzione e gli adattamenti tecnici necessari per il buon funzionamento del sistema. Tali compiti comprendono anche il coordinamento, la gestione e il sostegno delle attività di collaudo per il SIS centrale e gli N.SIS che garantiscono che il SIS centrale e gli N.SIS operino secondo i requisiti tecnici e funzionali di cui all'articolo 9.

8. La Commissione adotta atti di esecuzione al fine di stabilire i requisiti tecnici dell'infrastruttura di comunicazione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

Articolo 16

Sicurezza – eu-LISA

1. L'eu-LISA adotta le misure necessarie, compresi un piano di sicurezza, un piano di continuità operativa e un piano di ripristino in caso di disastro per il SIS centrale e l'infrastruttura di comunicazione, al fine di:

   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 dei dati personali (controllo all'ingresso delle installazioni);

c) impedire che i supporti di dati siano letti, copiati, modificati o rimossi 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 sistemi automatizzati di trattamento dei dati mediante apparecchiature per la trasmissione di dati (controllo degli utenti);

f) impedire che i dati siano trattati nel SIS senza autorizzazione e che i dati trattati nel SIS siano modificati o cancellati senza autorizzazione (controllo dell'inserimento dei dati);

g) garantire che le persone autorizzate a usare un sistema automatizzato di trattamento dei dati possano accedere solo ai dati previsti dalla loro autorizzazione di accesso attraverso identificatori di utente individuali e unici ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);

h) 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 a richiesta di quest'ultimo (profili del personale);

i) garantire la possibilità di verificare e accertare a quali organismi possano essere trasmessi dati personali mediante apparecchiature per la trasmissione di dati (controllo della trasmissione);

j) garantire la possibilità di verificare e accertare a posteriori quali dati personali siano stati introdotti nei sistemi automatizzati di trattamento dei dati, il momento dell'inserimento e la persona che lo ha effettuato (controllo dell'inserimento);

k) 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);

l) 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);

m) garantire che, in caso di interruzione delle operazioni, i sistemi installati possano essere ripristinati(ripristino);

n) garantire che il SIS esegua le sue funzioni correttamente, che gli errori siano segnalati (affidabilità) e che i dati personali conservati nel SIS non possano essere falsati da un errore di funzionamento del sistema (integrità); e

o) garantire la sicurezza dei suoi siti tecnici.

2. L'eu-LISA adotta misure equivalenti a quelle del paragrafo 1 per quanto riguarda la sicurezza dell'elaborazione e degli scambi di informazioni supplementari attraverso l'infrastruttura di comunicazione.

Articolo 17

Riservatezza – eu-LISA

1. Fatto salvo l'articolo 17 dello statuto dei funzionari, l'eu-LISA 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, secondo standard equiparabili a quelli previsti dall'articolo 11 del presente regolamento. Tale obbligo vincola gli interessati anche dopo che hanno lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

2. L'eu-LISA 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.

3. Se collabora con contraenti esterni per un qualsiasi compito relativo al SIS, l'eu-LISA monitora attentamente le attività del contraente per garantire il rispetto di tutte le disposizioni del presente regolamento, in particolare per quanto concerne la sicurezza, la riservatezza e la protezione dei dati.

4. La gestione operativa del CS-SIS non può essere affidata a imprese o organizzazioni private.

Articolo 18

Tenuta dei registri a livello centrale

1. L'eu-LISA provvede affinché ogni accesso a dati personali e ogni scambio dei medesimi nell'ambito del CS-SIS siano registrati ai fini di cui all'articolo 12, paragrafo 1.

2. I registri riportano, in particolare, la cronistoria della segnalazione, la data e l'ora dell'attività di trattamento dei dati, i dati usati per effettuare un'interrogazione, un riferimento ai dati trattati e gli identificatori di utente individuali e unici dell'autorità competente che effettua il trattamento dei dati.

3. In deroga al paragrafo 2 del presente articolo, se l'interrogazione è effettuata con dati dattiloscopici o un'immagine del volto in conformità dell'articolo 33, i registri riportano il tipo di dati usati per effettuare l'interrogazione anziché i dati effettivi.

4. I registri sono utilizzati solo ai fini di cui al paragrafo 1 e sono cancellati tre anni dopo la loro creazione. I registri contenenti la cronistoria delle segnalazioni sono cancellati tre anni dopo la cancellazione delle segnalazioni.

5. I registri possono essere tenuti più a lungo del termine di cui al paragrafo 4 se necessari per procedure di controllo già in corso.

6. Ai fini dell'autocontrollo e per garantire il corretto funzionamento del CS-SIS nonché l'integrità e la sicurezza dei dati, l'eu-LISA ha accesso a tali registri nei limiti delle sue competenze.

Il Garante europeo della protezione dei dati ha accesso a tali registri, nei limiti delle sue competenze e su sua richiesta, ai fini dell'assolvimento dei suoi compiti.

Capo IV
Informazione del pubblico

Articolo 19

Campagne d'informazione sul SIS

All'inizio dell'applicazione del presente regolamento, la Commissione, in collaborazione con le autorità di controllo e con il Garante europeo della protezione dei dati, effettua una campagna per informare il pubblico sugli obiettivi del SIS, sui dati ivi conservati, sulle autorità che hanno accesso al SIS e sui diritti degli interessati. La Commissione ripete siffatte campagne a intervalli regolari in collaborazione con le autorità di controllo e con il Garante europeo della protezione dei dati. La Commissione mantiene un sito web a disposizione del pubblico attraverso cui fornire tutte le informazioni pertinenti relative al SIS. Gli Stati membri, in collaborazione con le rispettive autorità di controllo, definiscono e attuano le politiche necessarie per informare i propri cittadini e residenti sul SIS in generale.

Capo V

Segnalazioni di cittadini di paesi terzi ai fini del respingimento e del rifiuto 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 contiene esclusivamente le categorie di dati forniti da ciascuno Stato membro che sono necessari ai fini previsti dagli articoli 24 e 25.

2. Le segnalazioni nel SIS che includono informazioni su persone contengono esclusivamente i seguenti dati:

   a) cognomi;

   b) nomi;

   c) nomi e cognomi alla nascita;

   d) nomi e cognomi precedenti e alias;

   e) segni fisici particolari, oggettivi ed inalterabili;

f) luogo di nascita;

g) data di nascita;

h) genere;

i) ogni cittadinanza posseduta;

j) l'indicazione che la persona:

   i) è armata;

   ii) è violenta;

   iii) è fuggita o evasa;

   iv) è a rischio suicidio;

   v) pone una minaccia per la salute pubblica; oppure

   vi) è coinvolta in un'attività di cui agli articoli da 3 a 14 della direttiva (UE) 2017/541;

k) ragione della segnalazione;

l) l'autorità autrice della segnalazione;

m) il riferimento alla decisione che ha dato origine alla segnalazione;

n) l'azione da intraprendere in caso di riscontro positivo (hit);

o) connessioni con altre segnalazioni a norma dell'articolo 48;

p) l'indicazione del fatto che la persona interessata è un familiare di un cittadino dell'Unione o di un'altra persona beneficiaria del diritto di libera circolazione a di cui all'articolo 26

q) l'indicazione del fatto che la decisione di respingimento e del rifiuto di soggiorno si fonda su uno degli elementi seguenti:

   i) precedente condanna di cui all'articolo 24, paragrafo 2, lettera a);

   ii) grave minaccia per la sicurezza di cui all'articolo 24, paragrafo 2, lettera b);

   iii) elusione della normativa dell'Unione o nazionale che disciplina l'ingresso e il soggiorno di cui all'articolo 24, paragrafo 2, lettera c);

   iv) divieto d'ingresso di cui all'articolo 24, paragrafo 1, lettera b); oppure

   v) provvedimento restrittivo di cui all'articolo 25;

r) tipo di reato;

s) categoria dei documenti di identificazione;

t) paese di rilascio dei documenti di identificazione;

u) numero dei documenti di identificazione;

v) data di rilascio dei documenti di identificazione;

w) fotografie e immagini del volto;

x) dati dattiloscopici;

y) copia, possibilmente a colori, dei documenti di identificazione.

3. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 2 del presente articolo e le norme comuni di cui al paragrafo 4 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

4. Le norme tecniche sono simili per le interrogazioni nel CS-SIS, nelle copie nazionali o condivise, e nelle copie tecniche di cui all'articolo 41, paragrafo 2. Tali norme devono essere basate su norme comuni.

Articolo 21

Proporzionalità

1. Prima di inserire una segnalazione e al momento di prolungare il periodo di validità di una segnalazione, lo Stato membro verifica se l'adeguatezza, la pertinenza e l'importanza del caso giustificano lla segnalazione nel SIS.

2. Nel caso in cui la decisione di respingimento e di rifiuto di soggiorno di cui all'articolo 24, paragrafo 1, lettera a), è connessa a un reato di terrorismo, il caso è ritenuto adeguato, pertinente e sufficientemente importante da giustificare la segnalazione nel SIS. Per motivi di sicurezza pubblica o 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

Requisito per inserire una segnalazione

1. L'insieme minimo di dati necessari per inserire una segnalazione nel SIS sono i dati di cui all'articolo 20, paragrafo 2, lettere a), g), k), m), n) e q). Gli altri dati di cui allo stesso paragrafo sono anch'essi inseriti nel SIS, se disponibili.

2. I dati di cui all'articolo 20, paragrafo 2, lettera e), del presente regolamento sono inseriti solo qualora ciò sia strettamente necessario ai fini dell'identificazione del cittadino di paese terzo interessato. Quando tali dati sono inseriti, gli Stati membri assicurano che l'articolo 9 del regolamento (UE) 2016/679 sia rispettato.

Articolo 23

Compatibilità delle segnalazioni

1. Prima di inserire una segnalazione, uno Stato membro verifica se la persona interessata sia già stata segnalata nel SIS. A tal fine, è effettuata anche una verifica con i dati dattiloscopici, se tali dati sono disponibili.

2. Per una stessa persona deve essere inserita nel SIS una sola segnalazione per Stato membro. Se necessario, possono essere inserite nuove segnalazioni sulla stessa persona da altri Stati membri, conformemente al paragrafo 3.

3. Quando una persona è già stata segnalata nel SIS, uno Stato membro che desideri inserire una nuova segnalazione verifica che non esista alcuna incompatibilità tra le segnalazioni. Se non vi è alcuna incompatibilità, lo Stato membro può inserire la nuova segnalazione. Se le segnalazioni sono incompatibili, gli uffici SIRENE degli Stati membri interessati si consultano tramite lo scambio di informazioni supplementari al fine di raggiungere un accordo. Le norme sulla compatibilità delle segnalazioni sono stabilite nel manuale SIRENE. Per motivi di interesse nazionale essenziale è possibile derogare alle norme sulla compatibilità previa consultazione tra gli Stati membri.

4. In caso di riscontri positivi (hit) su segnalazioni multiple di una stessa persona, lo Stato membro di esecuzione si conforma alle norme in materia di priorità delle segnalazioni previste nel manuale SIRENE.

Nel caso in cui una persona sia oggetto di segnalazioni multiple inserite da diversi Stati membri, le segnalazioni per l'arresto inserite conformemente all'articolo 26 del regolamento (UE) 2018/...[+] sono eseguite in via prioritaria a norma dell'articolo 25 di detto regolamento.

Articolo 24

Condizioni per inserire la segnalazione ai fini del respingimento o del rifiuto di soggiorno

1. Gli Stati membri inseriscono una segnalazione ai fini del respingimento e del rifiuto di soggiorno quando è soddisfatta una delle seguenti condizioni:

a) lo Stato membro ha concluso, alla luce di una valutazione individuale comprendente anche una valutazione delle circostanze personali del cittadino di paese terzo interessato e delle conseguenze di un respingimento e di un rifiuto di soggiorno, che la presenza di tale cittadino di paese terzo interessato nel proprio territorio costituisce una minaccia per l'ordine pubblico, la sicurezza pubblica o la sicurezza nazionale e, pertanto, ha adottato una decisione giudiziaria o amministrativa in conformità della normativa nazionale ai fini del respingimento e del rifiuto di soggiorno e ha emesso una segnalazione nazionale per gli stessi fini, oppure

b) lo Stato membro ha emesso un divieto d'ingresso secondo procedure conformi alla direttiva 2008/115/CE nei confronti di un cittadino di paese terzo.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 36/18.

2. Le situazioni di cui al paragrafo 1, lettera a), si verificano quando:

a) il cittadino di paese terzo è stato riconosciuto colpevole in uno Stato membro di un reato che comporta una pena detentiva di almeno un anno;

b) esistono fondati motivi per ritenere che il cittadino di paese terzo abbia commesso un reato grave, compreso un reato di terrorismo, o esistono indizi concreti della sua intenzione di commettere un tale reato nel territorio di uno Stato membro;

oppure

c) il cittadino di paese terzo ha eluso o tentato di eludere la normativa dell'Unione o nazionale che disciplina l'ingresso e il soggiorno nel territorio degli Stati membri.

3. Lo Stato membro segnalante provvede a che la segnalazione abbia effetto nel SIS non appena il cittadino di paese terzo interessato lascia il territorio degli Stati membri o non appena possibile qualora lo Stato membro segnalante riceva chiare indicazioni del fatto che il cittadino di paese terzo ha lasciato il territorio degli Stati membri al fine di impedire il reingresso di tale cittadino di paese terzo.

4. Le persone nei cui confronti sia stata emessa una decisione di respingimento e di rifiuto di soggiorno, come indicato al paragrafo 1, hanno il diritto di proporre ricorso. Tali ricorsi sono disciplinati conformemente alla normativa dell'Unione o nazionale, i quali forniscono un ricorso effettivo dinanzi a un giudice.

Articolo 25

Condizioni per l'inserimento della 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, 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 o alle segnalazioni inserite a norma del presente regolamento, la competenza spetta allo Stato membro che esercita la presidenza successiva e che ha accesso al SIS e alle segnalazioni inserite in conformità del presente regolamento.

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

Articolo 26

Condizioni per l'inserimento della segnalazione

di cittadini di paesi terzi beneficiari del diritto di libera circolazione nell'Unione

1. La segnalazione di un cittadino di paese terzo beneficiario del diritto di libera circolazione nell'Unione ai sensi della direttiva 2004/38/CE o di un accordo tra l'Unione o l'Unione e i suoi Stati membri, da un lato, e un paese terzo, dall'altro, è conforme alle norme adottate in attuazione di detta direttiva o dell'accordo.

2. In caso di riscontro positivo (hit) su una segnalazione inserita ai sensi dell'articolo 24 relativa a un cittadino di paese terzo beneficiario del diritto di libera circolazione nell'Unione, lo Stato membro di esecuzione consulta immediatamente lo Stato membro segnalante, tramite scambio di informazioni supplementari, al fine di decidere senza indugio l'azione da intraprendere.

Articolo 27

Consultazione preventiva prima del rilascio o della proroga di un permesso di soggiorno o di un visto per soggiorno di lunga durata

Qualora uno Stato membro esamini la possibilità di rilasciare o di prorogare un permesso di soggiorno o un visto per soggiorno di lunga durata ad un cittadino di paese terzo oggetto di una segnalazione ai fini del respingimento e del rifiuto di soggiorno inserita da un altro Stato membro, gli Stati membri interessati si consultano, tramite lo scambio di informazioni supplementari, in conformità delle disposizioni seguenti:

a) lo Stato membro di rilascio consulta lo Stato membro segnalante prima di rilasciare o prorogare il permesso di soggiorno o il visto per soggiorno di lunga durata;

b) lo Stato membro segnalante risponde alla richiesta di consultazione entro dieci giorni di calendario;

c) l'assenza di risposta entro il termine di cui alla lettera b) implica che lo Stato membro segnalante non si oppone al rilascio o alla proroga del permesso di soggiorno o del visto per soggiorno di lunga durata;

d) al momento di adottare la decisione pertinente, lo Stato membro di rilascio tiene conto dei motivi alla base della decisione dello Stato membro segnalante e prende in considerazione, in conformità della legislazione nazionale, ogni eventuale minaccia per l'ordine pubblico o la sicurezza pubblica che la presenza del cittadino di paese terzo in questione può porre nel territorio degli Stati membri;

e) lo Stato membro di rilascio comunica la sua decisione allo Stato membro segnalante; e

f) se lo Stato membro di rilascio comunica allo Stato membro segnalante la sua intenzione o la sua decisione di rilasciare o prorogare il permesso di soggiorno o il visto per soggiorno di lunga durata, lo Stato membro segnalante cancella la segnalazione ai fini del respingimento e del rifiuto di soggiorno.

La decisione finale di rilasciare a un cittadino di paese terzo il permesso di soggiorno o il visto per soggiorno di lunga durata spetta allo Stato membro di rilascio.

Articolo 28

Consultazione preliminare prima dell'inserimento di una segnalazione ai fini del respingimento e del rifiuto di soggiorno

Qualora uno Stato membro abbia adottato la decisione di cui all'articolo 24, paragrafo 1, ed esamini la possibilità di inserire una segnalazione ai fini del respingimento e del rifiuto di soggiorno per un cittadino di paese terzo che è titolare di un permesso di soggiorno o di un visto per soggiorno di lunga durata validi rilasciati da un altro Stato membro, gli Stati membri interessati si consultano, tramite lo scambio di informazioni supplementari, in conformità delle disposizioni seguenti:

a) lo Stato membro che ha adottato la decisione di cui all'articolo 24, paragrafo 1, informa lo Stato membro di rilascio in merito alla decisione;

b) le informazioni scambiate ai sensi della lettera a) del presente articolo contengono dettagli sufficienti sui motivi alla base della decisione di cui all'articolo 24, paragrafo 1;

c) sulla base delle informazioni fornite dallo Stato membro che ha adottato la decisione di cui all'articolo 24, paragrafo 1, lo Stato membro di rilascio valuta se vi siano motivi per revocare il permesso di soggiorno o il visto per soggiorno di lunga durata;

d) al momento di adottare la decisione pertinente, lo Stato membro di rilascio tiene conto dei motivi alla base della decisione dello Stato membro che ha adottato la decisione di cui all'articolo 24, paragrafo 1, e prende in considerazione, in conformità della legislazione nazionale, ogni eventuale minaccia per l'ordine pubblico o la sicurezza pubblica che la presenza del cittadino di paese terzo in questione può porre nel territorio degli Stati membri;

e) entro 14 giorni di calendario dal ricevimento della richiesta di consultazione, lo Stato membro di rilascio comunica la sua decisione allo Stato membro che ha adottato la decisione di cui all'articolo 24, paragrafo 1, o, se non è stato possibile adottare una decisione entro tale termine da parte dello stato di rilascio, gli rivolge una richiesta motivata di prorogare eccezionalmente i termini di risposta per un massimo di altri 12 giorni di calendario;

f) qualora lo Stato membro di rilascio comunichi allo Stato membro che ha adottato la decisione di cui all'articolo 24, paragrafo 1, di mantenere il permesso di soggiorno o il visto per soggiorno di lunga durata, lo Stato membro che ha adottato la decisione non inserisce la segnalazione ai fini del respingimento e del rifiuto di soggiorno.

Articolo 29

Consultazione a posteriori dopo l'inserimento di una segnalazione ai fini del respingimento e del rifiuto di soggiorno

Qualora risulti che uno Stato membro abbia inserito una segnalazione ai fini del respingimento e del rifiuto di soggiorno per un cittadino di paese terzo che è titolare di un permesso di soggiorno o di un visto per soggiorno di lunga durata validi rilasciati da un altro Stato membro, gli Stati membri interessati si consultano, tramite lo scambio di informazioni supplementari, in conformità delle disposizioni seguenti:

a) lo Stato membro segnalante informa lo Stato membro di rilascio in merito alla segnalazione ai fini del respingimento e del rifiuto di soggiorno;

b) le informazioni scambiate di cui alla lettera a) includono dettagli sufficienti sui motivi alla base della segnalazione ai fini del respingimento e del rifiuto di soggiorno;

c) lo Stato membro di rilascio valuta, sulla base delle informazioni fornite dallo Stato membro segnalante, se vi siano motivi per revocare il permesso di soggiorno o il visto per soggiorno di lunga durata;

d) al momento di adottare la decisione, lo Stato membro di rilascio tiene conto dei motivi alla base della decisione dello Stato membro segnalante e prende in considerazione, in conformità della legislazione nazionale, ogni eventuale minaccia per l'ordine pubblico o la sicurezza pubblica che la presenza del cittadino di paese terzo in questione può porre nel territorio degli Stati membri;

e) entro 14 giorni di calendario dal ricevimento della richiesta di consultazione, lo Stato membro di rilascio comunica allo Stato membro segnalante la sua decisione o, se non è stato possibile per lo Stato membro di rilascio adottare una decisione entro tale termine, gli rivolge una richiesta motivata di proroga dei termini di risposta; i termini possono essere eccezionalmente prorogati per un massimo di altri 12 giorni di calendario;

f) qualora lo Stato membro di rilascio comunichi allo Stato membro segnalante di mantenere il permesso di soggiorno o il visto per soggiorno di lunga durata, lo Stato membro segnalante cancella immediatamente la segnalazione ai fini del respingimento e del rifiuto di soggiorno.

Articolo 30

Consultazione in caso di riscontro positivo (hit) riguardante un cittadino di paese terzo titolare di un permesso di soggiorno o di un visto per soggiorno di lunga durata validi

Qualora uno Stato membro constati un riscontro positivo (hit) su una segnalazione ai fini del respingimento e del rifiuto di soggiorno inserita da uno Stato membro e riguardante un cittadino di paese terzo che è titolare di un permesso di soggiorno o di un visto per soggiorno di lunga durata validi rilasciati da un altro Stato membro, gli Stati membri interessati si consultano attraverso lo scambio di informazioni supplementari in conformità delle disposizioni seguenti:

a) lo Stato membro di esecuzione informa lo Stato membro segnalante in merito alla situazione,

b) lo Stato membro segnalante avvia la procedura di cui all'articolo 29;

c) lo Stato membro segnalante comunica allo Stato membro di esecuzione l'esito della consultazione.

La decisione riguardante l'ingresso del cittadino di paese terzo è adottata dallo Stato membro di esecuzione in conformità del regolamento (UE) 2016/399.

Articolo 31

Statistiche

Ogni anno gli Stati membri forniscono all'eu-LISA statistiche annuali sugli scambi di informazioni effettuati ai sensi degli articoli da 27 a 30 e sui casi in cui i termini non sono stati rispettati.

Capo VI
Interrogazione con dati biometrici

Articolo 32

Norme specifiche per inserire fotografie, immagini del volto e dati dattiloscopici

1. Sono inseriti nel SIS unicamente le fotografie, le immagini del volto e i dati dattiloscopici di cui all'articolo 20, paragrafo 2, lettere w) e x) che soddisfano norme minime di qualità dei dati e specifiche tecniche. Tali dati sono inseriti solo previo controllo di qualità volto ad accertare che siano state soddisfatte le norme minime di qualità dei dati e le specifiche tecniche.

2. I dati dattiloscopici inseriti nel SIS possono essere costituiti da una a dieci impronte digitali piane e da una a dieci impronte digitali rollate. Possono inoltre includere due impronte palmari.

3. Per l'archiviazione dei dati biometrici di cui al paragrafo 1 del presente articolo sono stabilite norme minime di qualità e specifiche tecniche in conformità del paragrafo 4 del presente articolo. Tali norme minime di qualità e specifiche tecniche stabiliscono il livello di qualità richiesto per l'uso dei dati ai fini della verifica dell'identità della persona in conformità dell'articolo 33, paragrafo 1, e per l'uso dei dati ai fini dell'identificazione della persona in conformità dell'articolo 33, paragrafi da 2 a 4.

4. La Commissione adotta atti di esecuzione al fine di stabilire le norme minime di qualità dei dati e le specifiche tecniche di cui ai paragrafi 1 e 3 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

Articolo 33

Norme specifiche per la verifica o l'interrogazione tramite fotografie, immagini del volto e dati dattiloscopici

1. Qualora siano disponibili fotografie, immagini del volto e dati dattiloscopici in una segnalazione nel SIS, tali fotografie, immagini del volto e dati dattiloscopici sono usati per confermare l'identità di una persona reperita grazie all'interrogazione del SIS con dati alfanumerici.

2. I dati dattiloscopici possono essere consultati in tutti i casi per identificare una persona. Tuttavia i dati dattiloscopici sono consultati a fini di identificazione di una persona se l'identità della persona non può essere accertata con altri mezzi. A tal fine il SIS centrale contiene un sistema automatico per il riconoscimento delle impronte digitali (AFIS).

3. I dati dattiloscopici nel SIS in relazione a segnalazioni inserite a norma degli articoli 24 e 25 possono essere consultati anche usando serie complete o incomplete di impronte digitali o palmari 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.

4. Non appena divenga tecnicamente possibile, e garantendo al contempo un grado elevato di affidabilità dell'identificazione, è possibile ricorrere a fotografie e immagini del volto per identificare una persona presso valichi di frontiera regolari.

Prima che questa funzionalità sia attuata nel SIS, la Commissione presenta una relazione sulla disponibilità, sullo stato di preparazione e sull'affidabilità della tecnologia necessaria. Il Parlamento europeo è consultato in merito alla relazione.

Dopo l'inizio dell'uso della funzionalità ai valichi di frontiera regolari, alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 61 per integrare il presente regolamento riguardo alla determinazione degli altri casi in cui è possibile ricorrere a fotografie e immagini del volto per identificare le persone.

Capo VII

Diritto di accesso e riesame e cancellazione delle segnalazioni

Articolo 34

Autorità competenti nazionali con diritto di accesso ai dati in SIS

1. Le autorità nazionali competenti responsabili dell'accertamento dell'identità dei cittadini di paesi terzi hanno accesso ai dati inseriti nel SIS e il diritto di consultarli direttamente o su una copia di dati SIS ai fini:

   a) dei controlli di frontiera, a norma del regolamento (UE) 2016/399;

   b) dei controlli di polizia e doganali effettuati all'interno dello Stato membro interessato e del relativo coordinamento da parte delle autorità designate;

   c) della prevenzione, dell'accertamento, dell'indagine o del perseguimento di reati di terrorismo o di altri reati gravi o dell'esecuzione di sanzioni penali, nello Stato membro interessato, purché si applichi la direttiva (UE) 2016/680;

d) dell'esame delle condizioni e dell'adozione di decisioni in materia di ingresso e soggiorno di cittadini di paesi terzi sul territorio degli Stati membri, compreso sui permessi di soggiorno e sui visti per soggiorni di lunga durata, e in materia di rimpatrio di cittadini di paesi terzi, nonché delle verifiche sui cittadini di paesi terzi che entrano o soggiornano illegalmente nel territorio degli Stati membri;

e) dei controlli di sicurezza sui cittadini di paesi terzi che chiedono la protezione internazionale, nella misura in cui le autorità che svolgono i controlli non siano "autorità accertanti" ai sensi dell'articolo 2, lettera f), della direttiva 2013/32/UE del Parlamento europeo e del Consiglio[1] e, se del caso, della consulenza fornita in conformità del regolamento (CE) n. 377/2004 del Consiglio[2];

f) dell'esame delle domande di visto e dell'assunzione delle relative decisioni, comprese le decisioni di annullamento, revoca o proroga del visto in conformità del regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio[3].

---

1 Direttiva 2013/32/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, recante procedure comuni ai fini del riconoscimento e della revoca dello status di protezione internazionale (GU L 180 del 29.6.2013, pag. 60).

2 Regolamento (CE) n. 377/2004 del Consiglio, del 19 febbraio 2004, relativo alla creazione di una rete di funzionari di collegamento incaricati dell'immigrazione (GU L 64 del 2.3.2004, pag. 1).

3 Regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, che istituisce un codice comunitario dei visti (codice dei visti) (GU L 243 del 15.9.2009, pag. 1).

2. Il diritto di accesso ai dati nel SIS e il diritto di consultarli direttamente possono essere esercitati dalle autorità nazionali competenti che sono responsabili della naturalizzazione, come previsto nella legislazione nazionale, ai fini dell'esame della domanda di naturalizzazione.

3. Ai fini degli articoli 24 e 25, il diritto di accesso ai dati presenti nel SIS e il diritto di consultarli direttamente possono essere esercitati anche dalle autorità giudiziarie nazionali, comprese quelle competenti per l'avvio dell'azione penale e per le indagini giudiziarie prima dell'imputazione, nell'assolvimento delle loro funzioni, come previsto nel diritto nazionale, e dalle relative autorità di coordinamento.

4. Il diritto di accesso ai dati riguardanti documenti su persone inseriti a norma dell'articolo 38, paragrafo 2, lettere k) e l), del regolamento (UE) 2018/...[+] e il diritto di consultarli possono essere esercitati anche dalle autorità di cui al paragrafo 1, lettera f) del presente articolo.

5. Le autorità competenti di cui al presente articolo sono inserite nell'elenco di cui all'articolo 41, paragrafo 8.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 36/18.

Articolo 35

Accesso di Europol ai dati nel SIS

1. L'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), istituita dal regolamento (UE) 2016/794, ove necessario all'adempimento del suo mandato, ha il diritto di accedere ai dati nel SIS e di consultarli. Europol può anche 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, 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 fornitele 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 di cui 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 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 solamente con il consenso dello Stato membro segnalante e in modo pienamente conforme alla normativa dell'Unione in materia di protezione dei dati.

5. Europol:

a) fatti salvi i paragrafi 4 e 6, non collega parti del SIS, né trasferisce i dati in esso contenuti cui ha accesso, a sistemi di raccolta e trattamento di dati gestiti da o presso Europol e non scarica o copia altrimenti parti del SIS;

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 ne fornisce una giustificazione;

c) limita l'accesso ai dati nel SIS, comprese le informazioni supplementari, al proprio personale specificamente autorizzato che necessita dell'accesso a tali dati per l'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 riceva una formazione e informazioni adeguate a norma dell'articolo 14, paragrafo 1; e

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 e di consultazione degli stessi e nello scambio e nel trattamento di informazioni supplementari.

6. Europol duplica i dati dal SIS soltanto per fini tecnici ove 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 solamente al fine di conservare i dati SIS 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. Europol non copia i dati di una segnalazione né i dati complementari trasmessi dagli Stati membri o dal CS-SIS negli altri sistemi di Europol.

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 e le interrogazioni del SIS in conformità dell'articolo 12. Tali registri e tale documentazione non sono considerati scaricamenti o duplicazioni illeciti di parti del SIS.

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 astenersi dall'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 36

Accesso ai dati nel SIS 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, i membri delle squadre ai sensi dell'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 34, paragrafo 1, del presente regolamento e abbiano ricevuto la formazione necessaria a norma dell'articolo 14, paragrafo 1, del presente regolamento il diritto di accedere ai dati inseriti nel SIS 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 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 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 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, 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 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 e le interrogazioni del SIS in conformità dell'articolo 12.

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. Nulla nel presente articolo può essere interpretato nel senso di pregiudicare 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 deidati.

7. Fatto salvo il paragrafo 2, nessuna parte del SIS 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 a cui hanno accesso tali squadre è trasferito a tale sistema. Nessuna parte del SIS può essere scaricata o duplicata. La registrazione degli accessi e delle interrogazioni non è considerata scaricamento illegale o duplicazione di dati SIS.

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 e di consultazione degli stessi. Ciò non pregiudica le ulteriori disposizioni del regolamento (UE) 2018/…[+].

Articolo 37

Valutazione dell'uso del SIS da parte di Europol e dell'Agenzia europea della guardia di frontiera e costiera

1. La Commissione effettua almeno ogni cinque anni una valutazione dell'esercizio e dell'uso del SIS da parte di Europol e delle squadre di cui all'articolo 36, paragrafo 1.

2. Europol e l'Agenzia europea della guardia di frontiera e costiera garantiscono un seguito adeguato alle conclusioni e alle raccomandazioni risultanti da tale valutazione.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 31/18.

3. Una relazione sui risultati della valutazione e sul relativo seguito è trasmessa al Parlamento europeo e al Consiglio.

Articolo 38

Ambito dell'accesso

Gli utenti finali, compresi Europol e i membri delle squadre ai sensi dell'articolo 2, punti 8) e 9), del regolamento (UE) 2016/1624, accedono solo ai dati necessari per l'assolvimento dei loro compiti.

Articolo 39

Periodo di riesame delle segnalazioni

1. Le segnalazioni sono conservate esclusivamente per il periodo necessario a realizzare le finalità per le quali sono state inserite.

2. Lo Stato membro segnalante riesamina la necessità di conservare una segnalazione entro tre anni dal suo inserimento nel SIS. Tuttavia se la decisione nazionale su cui si basa la segnalazione prevede un periodo di validità superiore a tre anni, la segnalazione è riesaminata entro cinque anni.

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

4. Nel periodo di riesame lo Stato membro segnalante può decidere, a seguito di una valutazione individuale globale che è registrata, di mantenere la segnalazione per un periodo più lungo del periodo di riesame, ove ciò sia necessario e proporzionato alle finalità per le quali la segnalazione stessa era stata inserita. In tal caso il paragrafo 2 si applica anche a tale proroga. Ogni proroga è comunicata 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 segnalante abbia informato il CS-SIS della proroga 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 redigono statistiche sul numero di segnalazioni il cui periodo di conservazione è stato prorogato a norma del paragrafo 4 del presente articolo e le trasmettono, su richiesta, alle autorità di controllo di cui all'articolo 55.

7. Non appena risulti chiaro all' ufficio SIRENE che una segnalazione ha conseguito il suo obiettivo e deve pertanto essere cancellata, l'ufficio SIRENE ne informa immediatamente l'autorità autrice della segnalazione. L'autorità dispone di 15 giorni di calendario dal ricevimento di tale comunicazione per rispondere che la segnalazione è stata o sarà cancellata, oppure indica i motivi della conservazione della segnalazione. In caso di mancata ricezione di una risposta alla scadenza del periodo di 15 giorni, l'ufficio SIRENE provvede affinché la segnalazione sia cancellata. Laddove consentito dalla legislazione nazionale, la segnalazione è cancellata dall'ufficio SIRENE. Gli uffici SIRENE segnalano alla rispettiva autorità di controllo i problemi ricorrenti incontrati nell'attività svolta ai sensi del presente paragrafo.

Articolo 40

Cancellazione delle segnalazioni

1. La segnalazione riguardante il respingimento e rifiuto di soggiorno ai sensi dell'articolo 24 è cancellata:

   a) allorché la decisione su cui si basava è stata revocata o annullata dall'autorità competente, oppure

   b) ove applicabile, in esito alla procedura di consultazione prevista dall'articolo 27 e dall'articolo 29.

2. La segnalazione di un cittadino di paese terzo oggetto di un provvedimento restrittivo diretto a impedirne l'ingresso o il transito nel territorio degli Stati membri è cancellata quando prende fine, è sospeso o è annullato il provvedimento restrittivo.

3. La segnalazione relativa alla persona che acquista la cittadinanza di uno Stato membro o di uno Stato i cui cittadini beneficiano del diritto di libera circolazione in virtù del diritto dell'Unione è cancellata non appena lo Stato membro segnalante viene a conoscenza o viene informato a norma dell'articolo 44 di tale acquisto.

4. Le segnalazioni sono cancellate alla loro scadenza ai sensi dell'articolo 39.

Capo VIII
Regole generali sul trattamento dei dati

Articolo 41

Trattamento dei dati del SIS

1. Gli Stati membri possono solo trattare i dati di cui all'articolo 20 ai fini del respingimento e del rifiuto di soggiorno nel loro territorio.

2. I dati sono duplicati soltanto per fini tecnici, sempreché tale duplicazione sia necessaria per la consultazione diretta da parte delle autorità competenti di cui all'articolo 34. Il presente regolamento si applicano a tali copie. Gli Stati membri non copiano i dati della segnalazione o i dati complementari inseriti da un altro Stato membro nel proprio N.SIS o nel CS-SIS.

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 48 ore.

   Nonostante il disposto del primo comma, non sono permesse copie tecniche che portino alla creazione di banche dati off-line ad uso delle autorità preposte al rilascio dei visti, 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 tengono un inventario aggiornato di tali copie, lo rendono accessibile alle rispettive autorità di controllo e assicurano che il presente regolamento, in particolare l'articolo 10, sia applicato a tali copie.

4. L'accesso ai dati del SIS da parte delle autorità competenti nazionali di cui all'articolo 34 è autorizzato esclusivamente nei limiti delle loro competenze e riservato solamente al personale debitamente autorizzato.

5. Ogni trattamento delle informazioni del SIS dagli Stati membri per finalità diverse da quelle per le quali vi sono state inserite deve essere connesso a un caso specifico e giustificato dalla necessità di prevenire una minaccia grave e imminente per l'ordine pubblico e la sicurezza pubblica, da fondati motivi di sicurezza nazionale o ai fini della prevenzione di un reato grave. A tale scopo è necessario ottenere l'autorizzazione preventiva dello Stato membro segnalante.

6. I dati riguardanti documenti su persone inseriti nel SIS a norma dell'articolo 38, paragrafo 2, lettere k) e l), del regolamento (UE) 2018/...[+] possono essere usati dalle autorità competenti di cui all'articolo 34, paragrafo 1, lettera f), conformemente alla legislazione di ciascuno Stato membro.

7. Qualsiasi uso dei dati del SIS non conforme ai paragrafi da 1 a 6 del presente articolo è considerato un abuso ai sensi della legislazione di ciascuno Stato membro ed è soggetto a sanzioni in conformità dell'articolo 59.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 36/18.

8. Ciascuno Stato membro invia all'eu-LISA l'elenco delle proprie autorità competenti autorizzate a consultare direttamente i dati nel SIS a norma del presente regolamento e le eventuali modifiche apportate all'elenco. L'elenco indica, per ciascuna autorità, i dati che essa può consultare e per quali finalità. L'eu-LISA provvede affinché l'elenco sia pubblicato nella *Gazzetta ufficiale dell'Unione europea* annualmente. L'eu-LISA mantiene sul proprio sito web un elenco sempre aggiornato contenente le modifiche trasmesse dagli Stati membri tra una pubblicazione annuale e l'altra.

9. Nella misura in cui il diritto dell'Unione non preveda specifiche disposizioni, la legislazione di ciascuno Stato membro si applica ai dati nel rispettivo N.SIS.

Articolo 42

Dati SIS e archivi nazionali

1. L'articolo 41, paragrafo 2, non pregiudica il diritto di uno Stato membro di conservare nel proprio archivio nazionale i dati SIS 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 41, paragrafo 2, non pregiudica il diritto di uno Stato membro di conservare nel proprio archivio nazionale i dati contenuti in una segnalazione particolare inserita nel SIS da quello stesso Stato membro.

Articolo 43

Informazione in caso di mancata esecuzione di una segnalazione

Se l'azione richiesta non può essere eseguita, lo Stato membro che ha richiesto l'intervento ne informa senza indugio lo Stato membro segnalante tramite lo scambio di informazioni supplementari.

Articolo 44

Qualità dei dati trattati nel SIS

1. Lo Stato membro segnalante è responsabile dell'esattezza e dell'attualità dei dati e della liceità del loro inserimento e della loro conservazione nel SIS.

2. Qualora uno Stato membro segnalante riceva pertinenti dati complementari o modificati di cui all'articolo 20, paragrafo 2, esso completa o modifica senza indugio la segnalazione.

3. Solo lo Stato membro segnalante è autorizzato a modificare, completare, rettificare, aggiornare o cancellare i dati che ha inserito nel SIS.

4. Qualora uno Stato membro diverso dallo Stato membro segnalante disponga di pertinenti dati complementari o modificati di cui all'articolo 20, paragrafo 2, esso li trasmette senza indugio, tramite lo scambio di informazioni supplementari, allo Stato membro segnalante per consentirgli di completare o modificare la segnalazione. I dati sono trasmessi solo se l'identità del cittadino di paese terzo è accertata.

5. Se uno Stato membro diverso dallo Stato membro segnalante è in possesso di elementi che dimostrano che detti dati contengono errori di fatto o sono stati archiviati illecitamente, ne informa al più presto, tramite lo scambio di informazioni supplementari ed entro due giorni lavorativi dacché è in possesso di detti elementi, lo Stato membro segnalante. Lo Stato membro segnalante verifica l'informazione e, se necessario, rettifica o cancella senza indugio i dati in questione.

6. Se, entro due mesi dal momento in cui sono emersi gli elementi ai sensi del paragrafo 5 del presente articolo gli Stati membri non giungono a un accordo, lo Stato membro che non ha inserito la segnalazione sottopone la questione alle autorità di controllo interessate e al Garante europeo della protezione dei dati affinché prendano una decisione mediante la cooperazione in conformità dell'articolo 57.

7. Gli Stati membri si scambiano informazioni supplementari nei casi in cui una persona presenti un ricorso nel quale faccia valere di non essere la persona oggetto della segnalazione. Se dalla verifica risulta che la persona oggetto della segnalazione è una persona distinta dal ricorrente, il ricorrente è informato delle disposizioni dell'articolo 47 e del suo diritto di ricorso di cui all'articolo 54, paragrafo 1.

Articolo 45

Incidenti di sicurezza

1. È considerato incidente di sicurezza qualunque evento che ha o possa avere ripercussioni sulla sicurezza del SIS o possa causare danni o perdite ai dati SIS o alle informazioni supplementari, in particolare quando possano essere stati consultati dati illecitamente o quando sono state o possano essere state compromesse la disponibilità, l'integrità e la riservatezza dei dati.

2. Gli incidenti di sicurezza sono gestiti in modo tale da garantire una risposta rapida, efficace e adeguata.

3. Fatte salve la notifica e la comunicazione di una violazione dei dati personali a norma dell'articolo 33 del regolamento (UE) 2016/679 o dell'articolo 30 della direttiva (UE) 2016/680, gli Stati membri, Europol e l'Agenzia europea della guardia di frontiera e costiera comunicano senza indugio gli incidenti di sicurezza alla Commissione, all'eu-LISA, all'autorità di controllo competente e al Garante europeo della protezione dei dati. L'eu-LISA comunica senza indugio qualsiasi incidente di sicurezza relativo al SIS centrale alla Commissione e al Garante europeo della protezione dei dati.

4. Le informazioni su un incidente di sicurezza che ha o possa avere ripercussioni sul funzionamento del SIS in uno Stato membro o nell'eu-LISA, o sulla disponibilità, integrità e riservatezza dei dati inseriti o inviati da altri Stati membri o sulle informazioni supplementari scambiate, sono trasmesse senza indugio a tutti gli Stati membri e registrate secondo il piano di gestione degli incidenti stabilito dall'eu-LISA.

5. Gli Stati membri e l'eu-LISA collaborano qualora si verifichino incidenti di sicurezza.

6. La Commissione segnala immediatamente al Parlamento europeo e al Consiglio gli incidenti gravi. Tali segnalazioni sono classificate EU RESTRICTED/RESTREINT UE conformemente alle norme vigenti in materia di sicurezza.

7. Qualora un incidente di sicurezza sia causato da un uso improprio dei dati, gli Stati membri, Europol e l'Agenzia europea della guardia di frontiera e costiera garantiscono l'imposizione di sanzioni in conformità dell'articolo 59.

Articolo 46

Distinzione tra persone con caratteristiche simili

1. Quando, inserendo una nuova segnalazione, risulta evidente che nel SIS è già presente una segnalazione nel SIS su una persona che possiede gli stessi elementi di descrizione dell'identità, l'ufficio SIRENE si mette in contatto entro 12 ore con lo Stato membro segnalante, tramite lo scambio di informazioni supplementari, allo scopo di verificare se la segnalazione riguardi o meno la stessa persona.

2. Se da tale controllo incrociato risulta che la persona oggetto di una nuova segnalazione e quella già inserita nel SIS sono effettivamente la stessa persona, l'ufficio SIRENE applica la procedura per l'inserimento di segnalazioni multiple di cui all'articolo 23.

3. Qualora la verifica stabilisca che si tratta di due persone diverse, l'ufficio SIRENE convalida la richiesta di inserimento della seconda segnalazione aggiungendo i dati necessari per evitare errori di identificazione.

Articolo 47

Dati complementari per trattare i casi di usurpazione di identità

1. Quando sono possibili confusioni fra la persona oggetto di una segnalazione e una persona la cui identità è stata usurpata, lo Stato membro segnalante aggiunge alla segnalazione, con il consenso esplicito della persona la cui identità è stata usurpata, dati che la riguardano per evitare le conseguenze negative di un errore di identificazione. La persona la cui identità sia stata usurpata ha il diritto di revocare il proprio consenso al trattamento dei dati personali aggiunti.

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 oggetto della segnalazione; e

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

3. Ai fini del presente articolo, e previo consenso esplicito della persona la cui identità è stata usurpata per ogni categoria di dati, possono essere inseriti e successivamente trattati nel SIS soltanto i seguenti dati personali della persona la cui identità è stata usurpata:

a) cognomi;

b) nomi;

c) nomi e cognomi alla nascita;

d) nomi e cognomi precedenti e alias, eventualmente registrati a parte;

e) segni fisici particolari, oggettivi e inalterabili;

f) luogo di nascita;

g) data di nascita;

h) genere;

i) fotografie e immagini del volto;

j) impronte digitali, impronte palmari o entrambe;

k) ogni cittadinanza posseduta;

l) categoria dei documenti di identificazione;

m) paese di rilascio dei documenti di identificazione;

n) numero dei documenti di identificazione;

o) data di rilascio dei documenti di identificazione;

p) indirizzo della persona;

q) nome del padre della persona;

r) nome della madre della persona.

4. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento e il successivo trattamento dei dati di cui al paragrafo 3 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

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. Esse possono accedervi all'unico scopo di evitare errori di identificazione.

Articolo 48

Connessioni fra segnalazioni

1. Uno Stato membro può creare una connessione tra le segnalazioni che introduce nel SIS. L'effetto della connessione è instaurare 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 periodo di riesame.

3. La creazione di una connessione non incide sui diritti di accesso previsti dal presente regolamento. 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 un'esigenza operativa.

5. Qualora uno Stato membro 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.

6. La Commissione adotta atti di esecuzione per stabilire e sviluppare norme tecniche necessarie per la connessione tra segnalazioni. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 62, paragrafo 2.

Articolo 49

Finalità e termini di conservazione delle informazioni supplementari

1. Gli Stati membri conservano un riferimento alle decisioni che danno origine a 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 le finalità per le quali sono stati forniti. Essi sono in ogni caso cancellati entro un anno dalla cancellazione dal SIS della relativa segnalazione.

3. Il paragrafo 2 non pregiudica il diritto dello Stato membro di conservare negli archivi nazionali i dati relativi a una determinata segnalazione da esso effettuata o a 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 disciplinato dalla legislazione nazionale.

Articolo 50

Trasferimento di dati personali a terzi

I dati trattati nel SIS e le relative informazioni supplementari scambiate a norma del presente regolamento non sono trasferiti a paesi terzi o ad organizzazioni internazionali, né sono messi a loro disposizione.

Capo IX
Protezione dei dati

Articolo 51

Legislazione applicabile

1. Il regolamento (UE) 2018/…[+] si applica al trattamento dei dati personali da parte dall'eu-LISA e dell'Agenzia europea della guardia di frontiera e costiera in conformità del presente regolamento. Il regolamento (UE) 2016/794 si applica al trattamento dei dati personali da parte di Europol in conformità del presente regolamento.

2. Il regolamento (UE) 2016/679 si applica al trattamento dei dati personali ai sensi del presente regolamento da parte delle autorità competenti di cui all'articolo 34 del presente regolamento, a eccezione del trattamento a fini di prevenzione, accertamento, indagine, o perseguimento di reati o esecuzione di sanzioni penali, comprese la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse, cui si applica la direttiva (UE) 2016/680.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 31/18.

Articolo 52

Diritto d'informazione

1. I cittadini di paesi terzi oggetto di una segnalazione nel SIS sono di ciò informati a norma degli articoli 13 e 14 del regolamento (UE) 2016/679 o degli articoli 12 e 13 della direttiva (UE) 2016/680. L'informazione è fornita per iscritto insieme a una copia della decisione nazionale che ha dato origine alla segnalazione di cui all'articolo 24, paragrafo 1, del presente regolamento, o a un riferimento a detta decisione.

2. L'informazione non è fornita 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, l'accertamento, l'indagine e il perseguimento di reati.

Articolo 53

Diritto di accesso, rettifica di dati inesatti e cancellazione di dati archiviati illecitamente

1. Gli interessati possono esercitare i diritti di cui agli articoli 15, 16 e 17 del regolamento (UE) 2016/679 e agli articoli 14, nonché 16, paragrafi 1 e 2, della direttiva (UE) 2016/680.

2. Uno Stato membro diverso dallo Stato membro segnalante può fornire a un interessato le informazioni su qualsiasi dato personale dell'interessato che viene trattatosoltanto se dà prima la possibilità allo Stato membro segnalante di prendere posizione. Alla comunicazione tra gli Stati membri si provvede tramite lo scambio di informazioni supplementari.

3. Gli Stati membri possono decidere di non fornire informazioni all'interessato, in tutto o in parte, in conformità della legislazione nazionale, nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi dell'interessato al fine di:

   a) non ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari;

   b) non compromettere la prevenzione, l'accertamento, l'indagine e il perseguimento di reati o l'esecuzione di sanzioni penali;

   c) proteggere la sicurezza pubblica;

   d) proteggere la sicurezza nazionale; oppure

   e) proteggere i diritti e le libertà altrui.

Nei casi di cui al primo comma, lo Stato membro informa l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione. Dette informazioni possono essere omesse qualora la loro comunicazione rischi di compromettere una delle finalità di cui al primo comma, lettere da a) a e). Lo Stato membro informa l'interessato della possibilità di proporre un reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale.

Lo Stato membro fornisce i motivi di fatto o di diritto su cui si basa la decisione di non fornire le informazioni all'interessato. Tali informazioni sono rese disponibili alle autorità di controllo.

In tali casi, l'interessato deve poter esercitare i propri diritti anche tramite le autorità di controllo competenti.

4. In seguito a una richiesta di accesso, rettifica o cancellazione, lo Stato membro informa l'interessato non appena possibile e comunque entro i termini di cui all'articolo 12, paragrafo 3, del regolamento (UE) 2016/679 del seguito dato all'esercizio dei diritti di cui al presente articolo, indipendentemente dal fatto che l'interessato sia presente o meno in un paese terzo.

Articolo 54

Mezzi di impugnazione

1. Fatte salve le disposizioni sui mezzi di impugnazione del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680, chiunque può adire qualsiasi autorità competente, tra cui un organo giurisdizionale, in base alla legislazione di qualsiasi Stato membro, per accedere, rettificare, cancellare, ottenere informazioni o per ottenere un indennizzo relativamente a una segnalazione che lo riguarda.

2. Gli Stati membri si impegnano reciprocamente ad eseguire le decisioni definitive emesse dai giudici o dalle autorità di cui al paragrafo 1 del presente articolo, fatto salvo l'articolo 58.

3. Gli Stati membri presentano relazioni annuali al comitato europeo per la protezione dei dati su:

   a) il numero di richieste di accesso presentate al titolare del trattamento e il numero di casi in cui è stato accordato l'accesso ai dati;

   b) il numero di richieste di accesso presentate all'autorità di controllo e il numero di casi in cui è stato accordato l'accesso ai dati;

   c) il numero di richieste di rettifica di dati inesatti e di cancellazione dei dati archiviati illecitamente che sono state presentate al titolare del trattamento e il numero di casi in cui i dati sono stati rettificati o cancellati;

d) il numero di richieste di rettifica di dati inesatti e di cancellazioni di dati archiviati illecitamente che sono state presentate all'autorità di controllo;

e) il numero di procedimenti giudiziari avviati;

f) il numero di cause in cui il giudice ha statuito a favore del ricorrente;

g) eventuali osservazioni sui casi di riconoscimento reciproco delle decisioni definitive emesse da giudici o autorità di altri Stati membri in merito a segnalazioni inserite dallo Stato membro segnalante.

Un modello per le relazioni di cui al presente paragrafo è elaborato dalla Commissione.

4. Le relazioni degli Stati membri sono incluse nella relazione congiunta di cui all'articolo 57, paragrafo 4.

Articolo 55

Controllo dell'N.SIS

1. Ogni Stato membro garantisce che le autorità di controllo indipendenti in esso designate e investite dei poteri di cui al capo VI del regolamento (UE) 2016/679 o al capo VI della direttiva (UE) 2016/680 controllino la liceità del trattamento dei dati personali nel SIS nel territorio di appartenenza e della loro trasmissione da detto territorio, nonché lo scambio e il successivo trattamento di informazioni supplementari nel territorio di appartenenza.

2. Le autorità di controllo provvedono affinché sia svolto un controllo delle operazioni di trattamento dei dati nel rispettivo N.SIS, conformemente alle norme di revisione internazionali, almeno ogni quattro anni. Il controllo è svolto dalle autorità di controllo oppure da queste commissionato direttamente a un revisore per la protezione di dati indipendente. Le autorità di controllo mantengono in qualsiasi momento il controllo sul revisore indipendente e la responsabilità del suo operato.

3. Gli Stati membri provvedono affinché le rispettive autorità di controllo dispongano delle risorse sufficienti per assolvere i compiti ad esse assegnati a norma del presente regolamento e possano avvalersi della consulenza di persone in possesso di adeguate conoscenze in materia di dati biometrici.

Articolo 56

Controllo dell'eu-LISA

1. Il Garante europeo della protezione dei dati ha il compito di sorvegliare le attività di trattamento dei dati personali da parte dell'eu-LISA e di assicurare che tali attività siano effettuate in conformità del presente regolamento. Si applicano di conseguenza i compiti e le competenze di cui agli articoli 57 e 58 del regolamento (UE) 2018/...[+].

2. Il Garante europeo della protezione dei dati svolge un controllo delle attività di trattamento dei dati personali effettuate dall'eu-LISA, conformemente alle norme di revisione internazionali, almeno ogni quattro anni. Una relazione su tale controllo è trasmessa al Parlamento europeo, al Consiglio, all'eu-LISA, alla Commissione e alle autorità di controllo. L'eu-LISA ha l'opportunità di presentare le sue osservazioni prima dell'adozione della relazione.

Articolo 57

Cooperazione tra le autorità di controllo
e il Garante europeo della protezione dei dati

1. Le autorità 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.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 31/18.

2. Le autorità di controllo e il comitato europeo per la protezione dei dati, ciascuno nell'ambito delle proprie competenze, essi si scambiano informazioni pertinenti, si assistono vicendevolmente nello svolgimento di revisioni e ispezioni, esaminano difficoltà di interpretazione o applicazione del presente regolamento e di altri atti giuridici dell'Unione applicabili, studiano i problemi emersi nell'esercizio di un controllo indipendente o nell'esercizio dei diritti degli interessati, elaborano proposte armonizzate per soluzioni congiunte di eventuali problemi e promuovono la sensibilizzazione del pubblico in materia di diritti di protezione dei dati.

3. Ai fini di cui al paragrafo 2, le autorità di controllo e il Garante europeo della protezione dei dati si incontrano almeno due volte l'anno nell'ambito del comitato europeo per la protezione dei dati. I costi di tali riunioni e la gestione delle stesse sono a carico del comitato europeo per la protezione dei dati. Nella prima riunione è adottato un regolamento interno. Ulteriori metodi di lavoro sono elaborati congiuntamente, se necessario.

4. Ogni anno il comitato europeo per la protezione dei dati trasmette al Parlamento europeo, al Consiglio e alla Commissione una relazione congiunta sulle attività inerenti al controllo coordinato.

Capo X
Responsabilità e sanzioni

Articolo 58
Responsabilità

1. Fatti salvi il diritto al risarcimento e ogni responsabilità ai sensi del regolamento (UE) 2016/679, della direttiva (UE) 2016/680 e del regolamento (UE) 2018/...[+]:

   a) ogni persona o Stato membro che abbia subito danni materiali o immateriali in conseguenza di un trattamento illecito di dati personali in seguito all'uso dell'N.SIS o di qualsiasi altro atto incompatibile con il presente regolamento compiuti da uno Stato membro ha diritto al risarcimento da parte di tale Stato membro; e

   b) ogni persona o Stato membro che abbia subito danni materiali o immateriali in conseguenza di qualsiasi atto incompatibile con il presente regolamento compiuto dall'eu-LISA ha diritto al risarcimento da parte della stessa.

   Uno Stato membro o l'eu-LISA sono esonerati in tutto o in parte da tale responsabilità di cui al primo comma se provano che l'evento che ha dato luogo al danno non è loro imputabile.

[+] GU: inserire il numero di serie del regolamento di cui al doc. PE-CONS 31/18.

2. Uno Stato membro è ritenuto responsabile di ogni eventuale danno arrecato al SIS conseguente all'inosservanza degli obblighi del presente regolamento, fatto salvo il caso e nella misura in cui l'eu-LISA o un altro Stato membro che partecipa al SIS abbiano omesso di adottare provvedimenti ragionevolmente idonei a prevenire il danno o ridurne al minimo l'impatto.

3. Le azioni proposte contro uno Stato membro per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono disciplinate dalla legislazione nazionale dello Stato membro. Le azioni proposte contro l'eu-LISA per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono soggette alle condizioni previste dai trattati.

Articolo 59

Sanzioni

Gli Stati membri provvedono affinché l'eventuale uso improprio dei dati SIS, od ogni trattamento di tali, o qualsiasi scambio di informazioni supplementari in contrasto con il presente regolamento sia punibile ai sensi della legislazione nazionale.

Le sanzioni previste sono effettive, proporzionate e dissuasive.

Capo XI
Disposizioni finali

Articolo 60

Controllo e statistiche

1. L'eu-LISA provvede affinché siano attivate procedure atte a controllare il funzionamento del SIS in rapporto agli obiettivi prefissati in termini di risultato, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

2. Ai fini della manutenzione tecnica, delle relazioni, delle relazioni sulla qualità dei dati, e delle statistiche, la eu-LISA ha accesso alle informazioni necessarie riguardanti le operazioni di trattamento effettuate nel SIS centrale.

3. L'eu-LISA pubblica statistiche giornaliere, mensili e annuali relative al numero di registrazioni per categoria di segnalazione, sia per ciascuno Stato membro sia su base aggregata. L'eu-LISA pubblica inoltre relazioni annuali relative al numero di riscontri positivi (hit) per categoria di segnalazione, al numero di interrogazioni del SIS e di accessi al SIS per l'inserimento, l'aggiornamento o la cancellazione di una segnalazione sia per ciascuno Stato membro sia su base aggregata. Tali statistiche includono statistiche sugli scambi di informazioni a norma degli articoli da 27 a 31. Le statistiche prodotte non contengono dati personali. La relazione statistica annuale è pubblicata.

4. Gli Stati membri, Europol e l'Agenzia europea della guardia di frontiera e costiera forniscono all'eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 3, 5, 7 e 8.

5. L'eu-LISA trasmette al Parlamento europeo, al Consiglio, agli Stati membri, alla Commissione, a Europol, all'Agenzia europea della guardia di frontiera e costiera nonché al Garante europeo della protezione dei dati tutte le relazioni statistiche che produce.

Per controllare l'attuazione degli atti giuridici nell'Unione, anche ai fini del regolamento (UE) n. 1053/2013, la Commissione può chiedere all'eu-LISA di fornire specifiche relazioni statistiche aggiuntive, periodicamente o ad hoc, sulle prestazioni del SIS, sull'uso del SIS e sullo scambio di informazioni supplementari.

L'Agenzia europea della guardia di frontiera e costiera può chiedere all'eu-LISA di fornire specifiche relazioni statistiche aggiuntive, periodicamente o ad hoc, ai fini dello svolgimento di analisi di rischio e valutazioni della vulnerabilità di cui agli articoli 11 e 13 del regolamento (UE) 2016/1624.

6. Ai fini dell'articolo 15, paragrafo 4, e dei paragrafi 3, 4 e 5 del presente articolo l'eu-LISA istituisce, attua e ospita un archivio centrale nei suoi siti tecnici contenente i dati di cui all'articolo 15, paragrafo 4, e al paragrafo 3 del presente articolo che non consentono l'identificazione delle persone fisiche e permettono alla Commissione e alle agenzie di cui paragrafo 5 del presente articolo di ottenere relazioni e statistiche personalizzate. Su richiesta, l'eu-LISA concede agli Stati membri, alla Commissione, a Europol e all'Agenzia europea della guardia di frontiera e costiera, nella misura necessaria all'assolvimento dei loro compiti, l'accesso all'archivio centrale mediante un accesso protetto tramite l'infrastruttura di comunicazione. L'eu-LISA pone in essere controlli dell'accesso e specifici profili di utente allo scopo di assicurare che all'archivio centrale si abbia accesso unicamente ai fini dell'elaborazione di relazioni e statistiche.

7. Due anni dopo la data di applicazione del presente regolamento a norma dell'articolo 66, paragrafo 5, primo comma e successivamente ogni due anni, l'eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sul funzionamento tecnico del SIS centrale e dell'infrastruttura di comunicazione, compresa la loro sicurezza, sull'AFIS e sullo scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri. Una volta la tecnologia in uso, la relazione contiene altresì una valutazione del ricorso alle immagini del volto per accertare l'identità delle persone.

8. Tre anni dopo la data di applicazione del presente regolamento a norma dell'articolo 66, paragrafo 5, primo comma e successivamente ogni quattro anni, la Commissione svolge una valutazione globale del SIS centrale e dello scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri. Tale valutazione globale comprende un'analisi dei risultati conseguiti in relazione agli obiettivi e una valutazione circa il perdurare della validità dei principi di base, l'applicazione del presente regolamento con riguardo al SIS centrale, la sicurezza del SIS centrale e le eventuali implicazioni per le attività future. La relazione di valutazione comprende altresì una valutazione dell'AFIS e delle campagne d'informazione sul SIS svolte dalla Commissione a norma dell'articolo 19.

La relazione di valutazione comprende anche statistiche sul numero di segnalazioni inserite ai sensi dell'articolo 24, paragrafo 1, lettera a) e statistiche sul numero di segnalazioni inserite ai sensi della lettera b) di tale paragrafo. Per quanto riguarda le segnalazioni l'articolo 24, paragrafo 1, lettera a), precisa quante segnalazioni sono state inserite a seguito delle situazioni di cui all'articolo 24, paragrafo 2, lettere a), b) o c). La relazione di valutazione comprende altresì una valutazione dell'applicazione dell'articolo 24 da parte degli Stati membri.

La Commissione trasmette la relazione di valutazione al Parlamento europeo e al Consiglio.

9. La Commissione adotta atti di esecuzione per stabilire le modalità dettagliate del funzionamento dell'archivio centrale di cui al paragrafo 6 del presente articolo e le norme sulla protezione dei dati e sulla sicurezza applicabili a tale archivio. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2.

Articolo 61

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 33, paragrafo 4, è conferito alla Commissione per un periodo indeterminato a decorrere dal ... [data di entrata in vigore del presente regolamento].

3. La delega di potere di cui all'articolo 33, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 33, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 62

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

Articolo 63

Modifiche al regolamento (CE) n. 1987/2006

Il regolamento (CE) n. 1987/2006 è così modificato:

1) l'articolo 6 è sostituito dal seguente:

"*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.";

2) l'articolo 11 è sostituito dal seguente:

"*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.

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.";

3) l'articolo 15 è così modificato:

a) è inserito il seguente paragrafo:

"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) il paragrafo 8 è sostituito dal seguente:

"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 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.";

4) all'articolo 17 sono aggiunti i paragrafi seguenti:

"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.";

5) all'articolo 20, paragrafo 2, è inserita la lettera seguente:

"k bis) tipo di reato;";

6) all'articolo 21, è aggiunto il paragrafo seguente:

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

7) l'articolo 22 è sostituito dal seguente:

"*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.";

8) l'articolo 26 è sostituito dal seguente:

"*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.";

9) sono inseriti gli articoli seguenti:

"*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*, 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 fornitele 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.

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.

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**, 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.

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/... del Parlamento europeo e del Consiglio***+.

---

* 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).

** 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).

*** Regolamento (UE) 2018/… del Parlamento europeo e del Consiglio 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 ...)".

+ GU: inserire il numero di serie nel testo e completare nella nota in calce il riferimento di pubblicazione del regolamento di cui al doc. PE-CONS 31/18.

Articolo 64

Modifica della convenzione di applicazione dell'accordo di Schengen

L'articolo 25 della convenzione di applicazione dell'accordo di Schengen è soppresso.

Articolo 65

Abrogazione

Il regolamento (CE) n. 1987/2006 è abrogato a decorrere dalla data di applicazione del presente regolamento di cui al primo comma dell'articolo 66, paragrafo 5.

I riferimenti al regolamento abrogato si intendono fatti al presente regolamento e si leggono secondo la tavola di concordanza di cui all'allegato.

Articolo 66

Entrata in vigore, inizio delle attività e applicazione

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

2. Al più tardi il ... [tre anni dopo l'entrata in vigore del presente regolamento] la Commissione adotta una decisione che stabilisce la data alla quale le attività del SIS hanno inizio a norma del presente regolamento, dopo aver verificato che sono soddisfatte le condizioni seguenti:

   a) sono stati adottati gli atti di esecuzione necessari per l'applicazione del presente regolamento;

   b) gli Stati membri hanno notificato alla Commissione di aver preso le disposizioni tecniche e giuridiche necessarie per trattare i dati SIS e scambiare informazioni supplementari a norma del presente regolamento; e

   c) l'eu-LISA ha comunicato alla Commissione il positivo completamento di tutte le attività di collaudo relative al CS-SIS e all'interazione tra CS-SIS e N.SIS.

3. La Commissione controlla attentamente il processo del graduale rispetto delle condizioni di cui al paragrafo 2 e informa il Parlamento europeo e il Consiglio in merito all'esito della verifica di cui a tale paragrafo.

4. Entro … [un anno dopo l'entrata in vigore del presente regolamento] e successivamente ogni anno fino all'adozione della decisione della Commissione di cui al paragrafo 2, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sullo stato di avanzamento per la preparazione della piena attuazione del presente regolamento. Tale relazione contiene anche informazioni particolareggiate sulle spese sostenute e sugli eventuali rischi che possono incidere sui costi complessivi.

5. Il presente regolamento si applica a decorrere dalla data stabilita in conformità del paragrafo 2.

In deroga al primo comma:

a) l'articolo 4, paragrafo 4, l'articolo 5, l'articolo 8, paragrafo 4, l'articolo 9, paragrafi 1 e 5, l'articolo 15, paragrafo 7, l'articolo 19, l'articolo 20, paragrafi 3 e 4, l'articolo 32, paragrafo 4, l'articolo 33, paragrafo 4, l'articolo 47, paragrafo 4, l'articolo 48, paragrafo 6, l'articolo 60, paragrafi 6 e 9, l'articolo 61, l'articolo 62, l'articolo 63, punti da 1) a 6) e punto 8), e i paragrafi 3 e 4 del presente articolo si applicano a decorrere dalla data di entrata in vigore del presente regolamento;

b) l'articolo 63, punto 9), si applica a decorrere da … [un anno dopo l'entrata in vigore del presente regolamento];

c) l'articolo 63, punto 7), si applica a decorrere da ... [due anni dopo l'entrata in vigore del presente regolamento].

6. La decisione della Commissione di cui al 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 conformemente ai trattati.

Fatto a Bruxelles,

Per il Parlamento europeo
Il presidente

Per il Consiglio
Il presidente

ALLEGATO

Tavola di concordanza

Regolamento (CE) n. 1987/2006	Il presente regolamento
Articolo 1	Articolo 1
Articolo 2	Articolo 2
Articolo 3	Articolo 3
Articolo 4	Articolo 4
Articolo 5	Articolo 5
Articolo 6	Articolo 6
Articolo 7	Articolo 7
Articolo 8	Articolo 8
Articolo 9	Articolo 9
Articolo 10	Articolo 10
Articolo 11	Articolo 11
Articolo 12	Articolo 12
Articolo 13	Articolo 13
Articolo 14	Articolo 14
Articolo 15	Articolo 15
Articolo 16	Articolo 16
Articolo 17	Articolo 17
Articolo 18	Articolo 18
Articolo 19	Articolo 19
Articolo 20	Articolo 20
Articolo 21	Articolo 21

Regolamento (CE) n. 1987/2006	Il presente regolamento
Articolo 22	Articoli 32 e 33
Articolo 23	Articolo 22
–	Articolo 23
Articolo 24	Articolo 24
Articolo 25	Articolo 26
Articolo 26	Articolo 25
–	Articolo 27
–	Articolo 28
–	Articolo 29
–	Articolo 30
–	Articolo 31
Articolo 27	Articolo 34
Articolo 27a	Articolo 35
Articolo 27b	Articolo 36
–	Articolo 37
Articolo 28	Articolo 38
Articolo 29	Articolo 39
Articolo 30	Articolo 40
Articolo 31	Articolo 41
Articolo 32	Articolo 42
Articolo 33	Articolo 43
Articolo 34	Articolo 44
–	Articolo 45
Articolo 35	Articolo 46

Regolamento (CE) n. 1987/2006	Il presente regolamento
Articolo 36	Articolo 47
Articolo 37	Articolo 48
Articolo 38	Articolo 49
Articolo 39	Articolo 50
Articolo 40	–
–	Articolo 51
Articolo 41	Articolo 53
Articolo 42	Articolo 52
Articolo 43	Articolo 54
Articolo 44	Articolo55
Articolo 45	Articolo 56
Articolo 46	Articolo 57
Articolo 47	–
Articolo 48	Articolo 58
Articolo 49	Articolo 59
Articolo 50	Articolo 60
–	Articolo 61
Articolo 51	Articolo 62
Articolo 52	–
–	Articolo 63
–	Articolo 64
Articolo 53	–
–	Articolo 65
Articolo 54	–
Articolo 55	Articolo 66