Gazzetta ufficiale dell'Unione europea

L 135

Edizione in lingua italiana

Legislazione

62° anno

22 maggio 2019

Sommario

IT

Gli atti i cui titoli sono stampati in caratteri chiari appartengono alla gestione corrente. Essi sono adottati nel quadro della politica agricola e hanno generalmente una durata di validità limitata.

I titoli degli altri atti sono stampati in grassetto e preceduti da un asterisco.

I

(Atti legislativi)

REGOLAMENTI

REGOLAMENTO (UE) 2019/816 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 aprile 2019

che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 82, paragrafo 1, secondo comma, lettera d),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria ([1]),

considerando quanto segue:

(1) L'Unione si è prefissa l'obiettivo di offrire ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone. Tale obiettivo dovrebbe essere conseguito, tra l'altro, attraverso misure appropriate per prevenire e combattere la criminalità, compresi la criminalità organizzata e il terrorismo.

(2) Detto obiettivo presuppone che le informazioni relative alle decisioni di condanna pronunciate negli Stati membri siano prese in considerazione al di fuori dello Stato membro di condanna, in occasione di un nuovo procedimento penale, come stabilito nella decisione quadro 2008/675/GAI del Consiglio ([2]), nonché per prevenire nuovi reati.

(3) Tale obiettivo implica lo scambio di informazioni estratte dal casellario giudiziale tra le competenti autorità degli Stati membri. Tale scambio di informazioni è organizzato e agevolato dalle norme fissate con decisione quadro 2009/315/GAI del Consiglio ([3]) e dal sistema europeo di informazione sui casellari giudiziali (ECRIS) istituito con decisione 2009/316/GAI del Consiglio ([4]).

(4) L'attuale quadro giuridico di ECRIS tuttavia non risponde sufficientemente alle caratteristiche delle richieste riguardanti cittadini di paesi terzi. Sebbene sia già possibile scambiare informazioni sui cittadini di paesi terzi tramite ECRIS, manca una procedura o un meccanismo comune dell'Unione che consenta di farlo in modo efficace, rapido e preciso.

(5) All'interno dell'Unione le informazioni sui cittadini di paesi terzi non sono raccolte come avviene per i cittadini degli Stati membri negli Stati membri di cittadinanza, ma sono solo conservate negli Stati membri in cui le condanne sono state pronunciate. Pertanto, per ottenere un quadro completo del trascorso criminale di un cittadino di paese terzo è necessario chiedere informazioni a tutti gli Stati membri.

([1]) Posizione del Parlamento europeo del 12 marzo 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 9 aprile 2019.

([2]) Decisione quadro 2008/675/GAI del Consiglio, del 24 luglio 2008, relativa alla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione di un nuovo procedimento penale (GU L 220 del 15.8.2008, pag. 32).

([3]) Decisione quadro 2009/315/GAI del Consiglio, del 26 febbraio 2009, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziale (GU L 93 del 7.4.2009, pag. 23).

([4]) Decisione 2009/316/GAI del Consiglio, del 6 aprile 2009, che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS) in applicazione dell'articolo 11 della decisione quadro 2009/315/GAI (GU L 93 del 7.4.2009, pag. 33).

(6) Tali «richieste generalizzate» impongono un onere amministrativo sproporzionato a tutti gli Stati membri, compresi quelli che non sono in possesso di informazioni sul cittadino di paese terzo interessato. Nella pratica tale onere scoraggia gli Stati membri dal chiedere agli altri Stati membri informazioni sui cittadini di paesi terzi, il che ostacola gravemente lo scambio di informazioni tra loro e fa sì che il loro accesso alle informazioni sui casellari giudiziali sia limitato a quelle conservate nei casellari nazionali. Di conseguenza, aumenta il rischio che lo scambio di informazioni tra Stati membri sia inefficiente e incompleto, il che si ripercuote a sua volta sul livello di sicurezza e protezione garantito ai cittadini dell'Unione e a quanti risiedono al suo interno.

(7) Per migliorare la situazione dovrebbe essere istituito un sistema che permetta all'autorità centrale di uno Stato membro di verificare con tempestività ed efficacia quali altri Stati membri siano in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo («ECRIS-TCN»). Il quadro ECRIS esistente potrebbe pertanto essere utilizzato per richiedere tali informazioni a quegli Stati membri conformemente alla decisione quadro 2009/315/GAI.

(8) Il presente regolamento dovrebbe pertanto prevedere le norme che istituiscono un sistema centralizzato a livello di Unione che contenga i dati personali, e le norme sulla ripartizione delle responsabilità tra gli Stati membri e sull'organizzazione responsabile dello sviluppo e della manutenzione del sistema centralizzato, come anche eventuali disposizioni specifiche in materia di protezione dei dati necessarie per integrare le disposizioni in vigore e per conseguire globalmente un livello adeguato di protezione e sicurezza dei dati e di salvaguardia dei diritti fondamentali degli interessati.

(9) Per conseguire l'obiettivo di offrire ai cittadini dell'Unione uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone, è altresì necessario disporre di informazioni complete per quanto riguarda le condanne a carico di cittadini dell'Unione che possiedono la cittadinanza di un paese terzo. Data la possibilità che tali persone si presentino in possesso di una o più cittadinanze e che negli Stati membri di condanna o nello Stato membro di cittadinanza siano registrate condanne diverse, è necessario includere nell'ambito di applicazione del presente regolamento i cittadini dell'Unione che possiedono anche la cittadinanza di un paese terzo. L'esclusione di tali persone risulterebbe nelle informazioni conservate in ECRIS-TCN rendendolo incompleto. Ciò pregiudicherebbe l'affidabilità del sistema. Tuttavia, poiché tali persone possiedono la cittadinanza dell'Unione, le condizioni per includere in ECRIS-TCN i dati relativi alle loro impronte digitali dovrebbero essere comparabili alle condizioni secondo cui gli Stati membri scambiano i dati relativi alle impronte digitali dei cittadini dell'Unione attraverso ECRIS, che è stato istituito dalla decisione quadro 2009/315/GAI e dalla decisione 2009/316/GAI. Pertanto, con riguardo ai cittadini dell'Unione che possiedono anche la cittadinanza di un paese terzo, i dati relativi alle impronte digitali dovrebbero essere inclusi in ECRIS-TCN soltanto se sono state rilevate in conformità del diritto nazionale durante un procedimento penale, fermo restando che, per tale inclusione, gli Stati membri dovrebbero poter utilizzare i dati relativi alle impronte digitali rilevati a fini diversi da un procedimento penale, qualora tale uso sia autorizzato dal diritto nazionale.

(10) ECRIS-TCN dovrebbe autorizzare il trattamento dei dati relativi alle impronte digitali allo scopo di individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo. Esso dovrebbe inoltre consentire il trattamento delle immagini del volto allo scopo di confermarne l'identità. È essenziale che l'inserimento e l'utilizzo dei dati relativi alle impronte digitali e delle immagini del volto non eccedano quanto strettamente necessario per raggiungere l'obiettivo perseguito, rispettino i diritti fondamentali, come pure l'interesse superiore del minore, e siano conformi alle norme applicabili dell'Unione in materia di protezione dei dati.

(11) All'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), istituita con regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio ([5]), dovrebbe essere affidato il compito di sviluppare e gestire ECRIS-TCN, in considerazione dell'esperienza che ha maturato nel gestire altri sistemi su larga scala nel settore della giustizia e degli affari interni. Ne dovrebbe essere modificato il mandato per tener conto di tali nuovi compiti.

(12) eu-LISA dovrebbe essere dotata di finanziamenti e personale adeguati per esercitare le sue responsabilità a norma del presente regolamento.

(13) Data la necessità di creare stretti collegamenti tecnici tra ECRIS-TCN ed ECRIS, a eu-LISA dovrebbe essere altresì affidato il compito di sviluppare ulteriormente e curare la manutenzione dell'implementazione di riferimento ECRIS, e il suo mandato dovrebbe essere modificato di conseguenza.

(14) Quattro Stati membri hanno sviluppato il proprio software nazionale di attuazione ECRIS conformemente alla decisione 2009/316/GAI e lo stanno utilizzando al posto dell'attuazione di riferimento ECRIS per lo scambio di informazioni estratte dai casellari giudiziali. Tenuto conto delle particolari caratteristiche che tali Stati membri hanno introdotto nei loro sistemi a uso nazionale e degli investimenti da loro effettuati, essi dovrebbero essere autorizzati a utilizzare i propri software nazionali di attuazione ECRIS ai fini di ECRIS-TCN, purché siano rispettate le condizioni di cui al presente regolamento.

([5]) Regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, 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 295 del 21.11.2018, pag. 99).

(15) ECRIS-TCN dovrebbe limitarsi a contenere le informazioni sull'identità dei cittadini di paesi terzi che sono stati condannati da una giurisdizione penale nell'Unione. Tali informazioni sull'identità dovrebbero comprendere dati alfanumerici e dati relativi alle impronte digitali. Dovrebbe altresì essere possibile includere le immagini del volto, nella misura in cui il diritto dello Stato membro in cui è stata pronunciata una condanna consenta di raccogliere e conservare le immagini del volto della persona condannata.

(16) È opportuno che i dati alfanumerici che gli Stati membri dovrebbero inserire nel sistema centrale includano il cognome e il nome o i nomi dell'interessato, nonché, se tali informazioni sono a disposizione dell'autorità centrale, eventuali pseudonimi o alias. Se lo Stato membro interessato è a conoscenza di altri dati personali differenti, come una grafia diversa di un nome in un altro alfabeto, dovrebbe essere possibile inserire tali dati potrebbero nel sistema centrale quali informazioni supplementari.

(17) I dati alfanumerici dovrebbero inoltre includere, quali informazioni supplementari, il numero di identità, o il tipo e il numero dei documenti di identificazione dell'interessato, nonché la denominazione dell'autorità che rilascia tali documenti, se tali informazioni sono a disposizione dell'autorità centrale. Lo Stato membro dovrebbe cercare di verificare l'autenticità dei documenti di identificazione prima di inserire le informazioni pertinenti nel sistema centrale. In ogni caso, dal momento che tali informazioni potrebbero non essere affidabili, è opportuno utilizzarle con cautela.

(18) Le autorità centrali dovrebbero usare ECRIS-TCN per individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo quando dette informazioni su tale persona sono richieste nello Stato membro in questione ai fini di un procedimento penale nei confronti di quella persona, oppure ai fini di cui al presente regolamento. Mentre ECRIS-TCN dovrebbe in linea di principio essere usato in tutti questi casi, l'autorità responsabile della conduzione di procedimenti penali dovrebbe poter decidere che ECRIS-TCN non debba essere usato quando non sia adeguato nelle circostanze del caso, per esempio, in alcuni tipi di procedimenti penali urgenti, nei casi di transito, nel caso in cui le informazioni sui casellari giudiziali siano state ottenute tramite ECRIS o in relazione a reati minori, in particolare le infrazioni minori in materia di circolazione, le violazioni minori dei regolamenti comunali generali e le violazioni minori dell'ordine pubblico.

(19) Gli Stati membri dovrebbero poter usare ECRIS-TCN anche per fini diversi da quelli stabiliti nel presente regolamento, se previsto conformemente al diritto nazionale. Tuttavia, per una maggiore trasparenza sull'uso di ECRIS-TCN, gli Stati membri dovrebbero notificare tali fini diversi alla Commissione, la quale dovrebbe provvedere alla pubblicazione di tutte le notifiche nella *Gazzetta ufficiale dell'Unione europea*.

(20) Dovrebbe altresì essere possibile per altre autorità che chiedono informazioni sui casellari giudiziali decidere che ECRIS-TCN non debba essere usato ove ciò non sia adeguato nelle circostanze del caso, per esempio quando devono essere effettuati determinati controlli amministrativi ordinari in merito alle qualifiche professionali di una persona, specie se è noto che non saranno richieste informazioni sui casellari giudiziali da altri Stati membri, a prescindere dal risultato dell'interrogazione di ECRIS-TCN. Tuttavia, ECRIS-TCN dovrebbe sempre essere usato quando la richiesta di informazioni sui casellari giudiziali proviene da una persona che chiede informazioni sul proprio casellario giudiziale, conformemente alla decisione quadro 2009/315/GAI, o quando è presentata per ottenere informazioni estratte dal casellario giudiziale conformemente alla direttiva 2011/93/UE del Parlamento europeo e del Consiglio ([6]).

(21) I cittadini di paesi terzi dovrebbero avere il diritto di ottenere per iscritto informazioni sul proprio casellario giudiziale ai sensi del diritto dello Stato membro nel quale presentano la richiesta e conformemente alla decisione quadro 2009/315/GAI del Consiglio. Prima di fornire tali informazioni a un cittadino di paese terzo, lo Stato membro interessato dovrebbe interrogare ECRIS-TCN.

(22) I cittadini dell'Unione che possiedono anche la cittadinanza di un paese terzo saranno inclusi in ECRIS-TCN soltanto se alle autorità competenti risulta che tali persone possiedono la cittadinanza di un paese terzo. Nel caso in cui alle autorità competenti non risulti che un cittadino dell'Unione possegga anche la cittadinanza di un paese terzo, è tuttavia possibile che la persona in questione sia stata oggetto di condanne precedenti in quanto cittadino di paese terzo. Per fare in modo che le autorità competenti abbiano un quadro completo dei casellari giudiziali, dovrebbe essere possibile interrogare ECRIS-TCN per verificare se, con riguardo a un cittadino dell'Unione, uno o più Stati membri siano in possesso di informazioni sul casellario giudiziale di tale persona in quanto cittadino di paese terzo.

(23) Qualora si verifichi una corrispondenza tra i dati registrati nel sistema centrale e i dati usati da uno Stato membro per interrogare il sistema (riscontro positivo), il sistema dovrebbe fornire insieme al riscontro positivo anche le informazioni sull'identità corrispondenti. Il risultato dell'interrogazione dovrebbe essere utilizzato dalle autorità centrali, al solo scopo di introdurre una richiesta tramite ECRIS o dall'Agenzia dell'Unione europea per la

([6]) Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

cooperazione giudiziaria penale (Eurojust), istituita dal regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio ([7]), dall'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), istituita dal regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ([8]), e dall'Ufficio pubblico ministero europeo («EPPO»), istituito dal regolamento (UE) n. 2017/1939 del Consiglio ([9]), al solo scopo di introdurre una richiesta di informazioni sulle condanne di cui al presente regolamento.

(24) In un primo tempo le immagini del volto incluse in ECRIS-TCN dovrebbero essere usate unicamente per confermare l'identità del cittadino di paese terzo allo scopo di individuare quali Stati membri siano in possesso di informazioni sulle condanne pronunciate a carico di tale cittadino di paese terzo. In futuro dovrebbe essere possibile utilizzare le immagini del volto in un confronto biometrico automatizzato, purché sussistano i requisiti previsti a tal fine a livello sia tecnico che politico. Tenuto conto di necessità e proporzionalità, nonché degli sviluppi tecnici nel settore del software di riconoscimento facciale, la Commissione dovrebbe valutare la disponibilità e lo stato di preparazione della tecnologia richiesta prima di adottare un atto delegato relativo all'uso delle immagini del volto per identificare i cittadini di paesi terzi, allo scopo di individuare quali Stati membri siano in possesso di informazioni sulle condanne pronunciate a carico di tali persone.

(25) Il ricorso ai dati biometrici è necessario in quanto è il metodo più affidabile per identificare i cittadini di paesi terzi presenti nel territorio degli Stati membri, che spesso sono sprovvisti di documenti o altro mezzo di identificazione, e per un confronto più affidabile tra i dati relativi a tali cittadini.

(26) Gli Stati membri dovrebbero inserire nel sistema centrale i dati relativi alle impronte digitali dei cittadini di paesi terzi condannati che sono stati rilevati conformemente al diritto nazionale nel corso di procedimenti penali. Per poter disporre, nel sistema centrale, di informazioni sull'identità quanto più complete possibile, gli Stati membri dovrebbero anche poter inserire nel sistema centrale i dati relativi alle impronte digitali che sono stati rilevati per fini diversi da un procedimento penale, qualora tali dati relativi alle impronte digitali siano disponibili per essere utilizzati in procedimenti penali conformemente al diritto nazionale.

(27) Il presente regolamento dovrebbe stabilire criteri minimi per quanto riguarda i dati relativi alle impronte digitali che gli Stati membri dovrebbero inserire nel sistema centrale. Agli Stati membri dovrebbe essere data la scelta tra l'inserimento dei dati relativi alle impronte digitali di cittadini di paesi terzi cui è stata comminata una pena detentiva di almeno sei mesi o l'inserimento dei dati relativi alle impronte digitali di cittadini di paesi terzi che sono stati condannati per un reato punibile conformemente al diritto dello Stato membro interessato con una pena detentiva della durata massima non inferiore a 12 mesi.

(28) Gli Stati membri dovrebbero creare in ECRIS-TCN registri di dati concernenti i cittadini di paesi terzi condannati. Ove possibile, ciò dovrebbe essere fatto automaticamente e senza ingiustificato ritardo dopo l'iscrizione della condanna nel casellario giudiziale nazionale. Gli Stati membri dovrebbero, conformemente al presente regolamento, inserire nel sistema centralizzato i dati alfanumerici e dati relativi alle impronte digitali relativamente alle condanne pronunciate dopo la data d'inizio dell'inserimento dei dati in ECRIN-TCN. A decorrere dalla stessa data, e in qualsiasi momento successivo, gli Stati membri dovrebbero poter inserire immagini del volto nel sistema centrale.

(29) Gli Stati membri dovrebbero altresì, a norma del presente regolamento, creare in ECRIS-TCN registri di dati concernenti i cittadini di paesi terzi condannati prima della data di inizio dell'inserimento dei dati, al fine di garantire la massima efficacia del sistema. Tuttavia, a tali fini non dovrebbe essere fatto obbligo agli Stati membri di raccogliere informazioni che non figuravano già nei rispettivi casellari giudiziali prima della data di inizio dell'inserimento dei dati. I dati relativi alle impronte digitali dei cittadini di paesi terzi raccolte in relazione a tali condanne precedenti dovrebbero essere incluse soltanto se sono state rilevate nel corso di procedimenti penali e se lo Stato membro interessato reputa possibile stabilire una chiara corrispondenza con altre informazioni sulle identità contenute nei casellari giudiziali.

(30) Un migliore scambio delle informazioni sulle condanne dovrebbe aiutare gli Stati membri nell'attuazione della decisione quadro 2008/675/GAI, che prescrive loro di prendere in considerazione le precedenti condanne in altri Stati membri nel corso di un nuovo procedimento penale, nella misura in cui le precedenti condanne a livello nazionale siano prese in considerazione conformemente al diritto nazionale.

([7]) Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, del 14 novembre 2018, che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio (GU L 295 del 21.11.2018, pag. 138).

([8]) 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).

([9]) Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO») (GU L 283 del 31.10.2017, pag. 1).

(31) Un riscontro positivo rilevato da ECRIS-TCN non dovrebbe di per sé implicare che il cittadino di paese terzo interessato è stato condannato negli Stati membri che sono indicati. La conferma che esistono precedenti condanne dovrebbe risultare unicamente dalle informazioni ricevute dai casellari giudiziali degli Stati membri interessati.

(32) Nonostante la possibilità di avvalersi di programmi finanziari dell'Unione in conformità delle norme applicabili, ogni Stato membro dovrebbe sostenere i propri costi per l'attuazione, la gestione, l'uso e la manutenzione delle banche dati nazionali di casellari giudiziali e di impronte digitali e per l'attuazione, la gestione, l'uso e la manutenzione degli adeguamenti tecnici necessari per usare ECRIS-TCN, comprese le connessioni al punto di accesso centrale nazionale.

(33) Eurojust, Europol ed EPPO dovrebbero avere accesso a ECRIS-TCN al fine di individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo, ai fini dello svolgimento dei loro compiti statutari. Eurojust dovrebbe inoltre avere accesso diretto a ECRIS-TCN ai fini dello svolgimento del proprio compito a norma del presente regolamento, di agire da punto di contatto per i paesi terzi e le organizzazioni internazionali, fatta salva l'applicazione dei principi della cooperazione giudiziaria in materia penale, incluse le norme sull'assistenza giudiziaria reciproca. Se, da un lato, è opportuno tenere conto della posizione degli Stati membri che non partecipano alla procedura di cooperazione rafforzata sull'istituzione dell'EPPO, dall'altro all'EPPO non dovrebbe essere negato l'accesso a informazioni relative alle condanne per il solo motivo che lo Stato membro interessato non partecipa a detta cooperazione rafforzata.

(34) Il presente regolamento stabilisce rigorose norme di accesso a ECRIS-TCN e le necessarie garanzie, compresa la responsabilità degli Stati membri nel raccogliere e usare i dati. Esso stabilisce inoltre le modalità con cui i singoli possono esercitare i loro diritti in materia di risarcimento, accesso, rettifica, cancellazione e ricorso, in particolare il diritto a un ricorso effettivo e il controllo del trattamento dei dati da parte di autorità pubbliche indipendenti. Il presente regolamento rispetta pertanto diritti e libertà fondamentali sanciti, in particolare, nella Carta dei diritti fondamentali dell'Unione europea, compresi il diritto alla protezione dei dati di carattere personale, il principio dell'uguaglianza davanti alla legge e il divieto generale di discriminazione. A tale proposito, esso tiene anche conto della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, del Patto internazionale relativo ai diritti civili e politici e degli altri obblighi di diritto internazionale in materia di diritti umani.

(35) La direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([10]) dovrebbe applicarsi al trattamento dei dati personali da parte delle autorità nazionali competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse. Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([11]) dovrebbe applicarsi al trattamento dei dati personali da parte delle autorità nazionali quando tale trattamento non rientra nell'ambito di applicazione della direttiva (UE) 2016/680. Dovrebbe essere assicurato il controllo coordinato a norma del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([12]), il quale dovrebbe applicarsi anche al trattamento dei dati personali da parte di eu-LISA.

(36) Per quanto riguarda le condanne precedenti, le autorità centrali dovrebbero inserire i dati alfanumerici entro la scadenza del termine per l'inserimento dei dati a norma del presente regolamento e i dati relativi alle impronte digitali entro due anni dalla data di entrata in funzione di ECRIS-TCN. Gli Stati membri dovrebbero poter inserire tutti i dati contemporaneamente, a condizione di rispettare tali termini.

(37) È opportuno stabilire norme relative alla responsabilità degli Stati membri, dell'Eurojust, di Europol, dell'EPPO e di eu-LISA per eventuali danni derivanti dalla violazione del presente regolamento.

(38) Per migliorare l'individuazione degli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea (TFUE) per integrare il presente regolamento prevedendo l'uso delle immagini del volto ai fini dell'identificazione di cittadini di paesi terzi in modo da individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate. È di particolare

([10]) 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).

([11]) 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).

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

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 ([13]). 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 degli atti delegati.

(39) Al fine di garantire condizioni uniformi per l'istituzione e la gestione operativa di ECRIS-TCN, dovrebbero essere attribuite alla Commissione competenze di esecuzione. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([14]).

(40) Gli Stati membri dovrebbero quanto prima adottare le misure necessarie per conformarsi al presente regolamento in modo da garantire il corretto funzionamento di ECRIS-TCN, tenuto conto del tempo necessario a eu-LISA per sviluppare e realizzare ECRIS-TCN. Tuttavia, gli Stati membri dovrebbero disporre almeno di 36 mesi dall'entrata in vigore del presente regolamento per adottare le misure necessarie a conformarvisi.

(41) Poiché l'obiettivo del presente regolamento, vale a dire consentire uno scambio rapido ed efficace di informazioni esatte estratte dal casellario giudiziale relative ai cittadini di paesi terzi, non può essere conseguito in misura sufficiente dagli Stati membri ma, attuando norme comuni, può essere conseguito 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 tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(42) 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.

(43) A norma degli articoli 1 e 2 e dell'articolo 4 *bis*, paragrafo 1, del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda non partecipa all'adozione del presente regolamento, non è da esso vincolata, né è soggetta alla sua applicazione.

(44) A norma dell'articolo 3 e dell'articolo 4 *bis*, paragrafo 1, del protocollo n. 21, il Regno Unito ha notificato che desidera partecipare all'adozione e all'applicazione del presente regolamento.

(45) 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 ([15]) e ha espresso un parere il 12 dicembre 2017 ([16]),

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPITOLO I

Disposizioni generali

Articolo 1

Oggetto

Il presente regolamento stabilisce:

a) un sistema per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi («ECRIS-TCN»);

b) le condizioni alle quali ECRIS-TCN è usato dalle autorità centrali al fine di ottenere informazioni su tali condanne precedenti attraverso il sistema europeo di informazione sui casellari giudiziali (ECRIS) istituito con decisione 2009/316/GAI, nonché le condizioni alle quali l'Eurojust, l'Europol e l'EPPO usano ECRIS-TCN.

([13]) GU L 123 del 12.5.2016, pag. 1.
([14]) 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).
([15]) 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).
([16]) GU C 55 del 14.2.2018, pag. 4.

Articolo 2

Ambito di applicazione

Il presente regolamento si applica al trattamento delle informazioni sull'identità di cittadini di paesi terzi che siano stati oggetto di condanne negli Stati membri, allo scopo di individuare gli Stati membri in cui sono state pronunciate tali condanne. A eccezione dell'articolo 5, paragrafo 1, lettera b), punto ii), le disposizioni del presente regolamento che si applicano ai cittadini di paesi terzi si applicano altresì ai cittadini dell'Unione che possiedono anche la cittadinanza di un paese terzo e sono stati oggetto di condanne negli Stati membri.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

1) «condanna», la decisione definitiva di una giurisdizione penale nei confronti di una persona fisica in relazione a un reato, nella misura in cui tale decisione sia riportata nel casellario giudiziale dello Stato membro di condanna;

2) «procedimento penale», la fase precedente al processo penale, la fase del processo penale stesso e l'esecuzione della condanna;

3) «casellario giudiziale», il registro nazionale o i registri nazionali in cui le condanne sono registrate conformemente al diritto nazionale;

4) «Stato membro di condanna», lo Stato membro in cui è stata pronunciata una condanna;

5) «autorità centrale», un'autorità designata conformemente all'articolo 3, paragrafo 1, della decisione quadro 2009/315/GAI;

6) «autorità competenti», le autorità centrali ed Eurojust, Europol ed EPPO che sono competenti per accedere a ECRIS-TCN o per interrogarlo a norma del presente regolamento;

7) «cittadino di paese terzo», chiunque non sia cittadino dell'Unione ai sensi dell'articolo 20, paragrafo 1, TFUE, l'apolide o qualsiasi persona la cui cittadinanza è ignota;

8) «sistema centrale», la banca o le banche dati, il cui sviluppo e la cui manutenzione fanno capo a eu-LISA, che detiene le informazioni sull'identità di cittadini di paesi terzi che sono stati oggetto di condanne negli Stati membri;

9) «software di interfaccia», il software ospitato dalle autorità competenti che consente loro di accedere al sistema centrale tramite l'infrastruttura di comunicazione di cui all'articolo 4, paragrafo 1, lettera d);

10) «informazioni sull'identità», i dati alfanumerici, i dati relativi alle impronte digitali e le immagini del volto utilizzati per stabilire una connessione tra tali dati e una persona fisica;

11) «dati alfanumerici», i dati rappresentati da lettere, cifre, caratteri speciali, spazi e segni di punteggiatura;

12) «dati relativi alle impronte digitali», i dati relativi alle impressioni piatte e rollate delle impronte digitali di ciascun dito di una persona;

13) «immagine del volto», le immagini digitalizzate del volto di una persona;

14) «riscontro positivo», la o le corrispondenze constatate, sulla base di un confronto, tra le informazioni sull'identità registrate nel sistema centrale e le informazioni sull'identità usate per interrogare il sistema;

15) «punto di accesso centrale nazionale», il punto nazionale di connessione all'infrastruttura di comunicazione di cui all'articolo 4, paragrafo 1, lettera d);

16) «implementazione di riferimento ECRIS», il software sviluppato dalla Commissione e messo a disposizione degli Stati membri per lo scambio delle informazioni sui casellari giudiziali tramite ECRIS;

17) «autorità nazionale di controllo», un'autorità pubblica indipendente istituita da uno Stato membro in conformità delle norme dell'Unione in materia di protezione dei dati;

18) «autorità di controllo», il Garante europeo della protezione dei dati e le autorità nazionali di controllo.

Articolo 4

Architettura tecnica di ECRIS-TCN

1. ECRIS-TCN consta di:

a) un sistema centrale in cui sono conservate le informazioni sull'identità dei cittadini di paesi terzi condannati;

b) un punto di accesso centrale nazionale in ciascuno Stato membro;

c) un software di interfaccia che connette le autorità competenti al sistema centrale tramite il punto di accesso centrale nazionale e l'infrastruttura di comunicazione di cui alla lettera d);

d) un'infrastruttura di comunicazione tra il sistema centrale e il punto di accesso centrale nazionale.

2. Il sistema centrale è ospitato da eu-LISA presso i suoi siti tecnici.

3. Il software di interfaccia è integrato con l'attuazione di riferimento ECRIS. Gli Stati membri usano l'attuazione di riferimento ECRIS o, nella situazione e alle condizioni di cui ai paragrafi da 4 a 8, il software nazionale di attuazione ECRIS, per interrogare ECRIS-TCN e per trasmettere le successive richieste di informazioni sui casellari giudiziali.

4. Gli Stati membri che utilizzano il proprio software nazionale di attuazione ECRIS sono tenuti a garantire che esso consenta alle loro autorità nazionali incaricate dei casellari giudiziali di utilizzare ECRIS-TCN, a eccezione del software di interfaccia, conformemente al presente regolamento. A tale scopo, prima della data di entrata in funzione di ECRIS-TCN ai sensi dell'articolo 35, paragrafo 4, essi garantiscono che il loro software nazionale di attuazione ECRIS funzioni conformemente ai protocolli e alle specifiche tecniche definite negli atti di esecuzione di cui all'articolo 10 e a eventuali altri requisiti tecnici definiti da eu-LISA ai sensi del presente regolamento basati su detti atti di esecuzione.

5. Fintanto che non usano l'attuazione di riferimento ECRIS, gli Stati membri che usano il proprio software nazionale di attuazione ECRIS garantiscono inoltre l'introduzione nel loro software nazionale di attuazione ECRIS dei successivi adattamenti tecnici resi necessari da eventuali modifiche delle specifiche tecniche definite negli atti di esecuzione di cui all'articolo 10 o da modifiche di eventuali altri requisiti tecnici definiti da eu-LISA ai sensi del presente regolamento basati su detti atti di esecuzione, senza ingiustificato ritardo.

6. Gli Stati membri che usano il proprio software nazionale di attuazione ECRIS sostengono tutte le spese associate all'attuazione, alla manutenzione e all'ulteriore sviluppo del loro software nazionale di attuazione ECRIS e alla sua interconnessione con ECRIS-TCN, con l'eccezione del software di interfaccia.

7. Qualora uno Stato membro che usa il proprio software di attuazione ECRIS non sia in grado di conformarsi agli obblighi di cui al presente articolo, ha l'obbligo di usare l'attuazione di riferimento ECRIS, incluso il software di interfaccia integrato, per avvalersi di ECRIS-TCN.

8. Alla luce della valutazione che la Commissione è tenuta a effettuare ai sensi dell'articolo 36, paragrafo 10, lettera b), gli Stati membri interessati forniscono alla Commissione tutte le informazioni necessarie.

CAPITOLO II

Inserimento e uso dei dati da parte delle autorità centrali

Articolo 5

Inserimento dei dati in ECRIS-TCN

1. Per ciascun cittadino di paese terzo condannato l'autorità centrale dello Stato membro di condanna crea una registrazione di dati nel sistema centrale. Tale registrazione di dati comprende:

a) per quanto riguarda i dati alfanumerici:

i) informazioni da includere a meno che, in singoli casi, tali informazioni non siano note all'autorità centrale (informazioni obbligatorie):

— cognome;

— nome o nomi;

— data di nascita;

— luogo di nascita (città e paese);

— la o le cittadinanze;

— sesso;

— nomi precedenti, se del caso;

— codice dello Stato membro di condanna;

ii) informazioni da includere se sono state inserite nel casellario giudiziale (informazioni facoltative):

— nome dei genitori;

iii) informazioni da includere se sono a disposizione dell'autorità centrale (informazioni supplementari):

— numero di identità, o tipo e numero del documento di identificazione dell'interessato, nonché denominazione dell'autorità di rilascio;

— eventuali pseudonimi o alias;

b) per quanto riguarda i dati relativi alle impronte digitali:

i) dati relativi alle impronte digitali che sono stati rilevati conformemente al diritto nazionale nel corso di procedimenti penali;

ii) come minimo, dati relativi alle impronte digitali rilevati in base a uno dei seguenti criteri:

— se il cittadino di paese terzo è stato condannato a una pena detentiva di almeno sei mesi;

o

— se il cittadino di paese terzo è stato condannato per un reato punibile, a norma del diritto dello Stato membro, con una pena detentiva della durata massima non inferiore a 12 mesi.

2. I dati relativi alle impronte digitali di cui al paragrafo 1, lettera b), del presente articolo devono soddisfare le specifiche tecniche per la qualità, la risoluzione e il trattamento dei dati relativi alle impronte digitali previste negli atti di esecuzione di cui all'articolo 10, paragrafo 1, lettera b). Il numero di riferimento dei dati relativi alle impronte digitali della persona condannata include il codice dello Stato membro di condanna.

3. La registrazione di dati può contenere anche le immagini del volto del cittadino di paese terzo condannato, qualora il diritto dello Stato membro di condanna consenta di raccogliere e conservare le immagini del volto delle persone condannate.

4. Lo Stato membro di condanna crea la registrazione di dati automaticamente, ove possibile, e senza ingiustificato ritardo dopo l'iscrizione della condanna nel casellario giudiziale.

5. Gli Stati membri di condanna creano inoltre la registrazione di dati per le condanne pronunciate prima della data di entrata in funzione dei dati ai sensi dell'articolo 35, paragrafo 1, nella misura in cui i dati relativi alle persone condannate sono conservati nelle loro banche dati nazionali. In tali casi i dati relativi alle impronte digitali devono essere inclusi soltanto se sono state rilevate nel corso di procedimenti penali conformemente al diritto nazionale e se è possibile stabilire una chiara corrispondenza con altre informazioni sull'identità contenute nei casellari giudiziali.

6. Al fine di rispettare gli obblighi di cui al paragrafo 1, lettera b), punti i) e ii), e al paragrafo 5, gli Stati membri possono utilizzare i dati relativi alle impronte digitali rilevate a fini diversi da un procedimento penale, qualora tale uso sia autorizzato dal diritto nazionale.

Articolo 6

Immagini del volto

1. Fino all'entrata in vigore dell'atto delegato di cui al paragrafo 2, le immagini del volto possono essere utilizzate al solo scopo di confermare l'identità del cittadino di paese terzo identificato grazie all'interrogazione con dati alfanumerici o con dati relativi alle impronte digitali.

2. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 37 al fine di integrare il presente regolamento per quanto riguarda l'uso delle immagini del volto ai fini dell'identificazione di cittadini di paesi terzi in modo da individuare, quando sarà possibile a livello tecnico, gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di tali persone. Prima di esercitare tale potere, la Commissione valuta, tenendo conto della necessità e della proporzionalità, nonché degli sviluppi tecnici nel settore del software di riconoscimento facciale, la disponibilità e lo stato di preparazione della tecnologia necessaria.

Articolo 7

Utilizzo di ECRIS-TCN per individuare gli Stati membri in possesso di informazioni sui casellari giudiziali

1. Le autorità centrali usano ECRIS-TCN per individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo, al fine di ottenere informazioni sulle precedenti condanne tramite ECRIS, quando dette informazioni su tale persona sono richieste nello Stato membro in questione ai fini di un procedimento penale nei confronti di quella persona o per uno qualsiasi dei seguenti fini, se previsto conformemente al diritto nazionale:

— permettere a una persona, su sua richiesta, di verificare il proprio casellario giudiziale;

— rilasciare nulla osta di sicurezza;

— ottenere una licenza o un permesso;

— effettuare indagini di sicurezza a fini occupazionali;

— effettuare indagini di sicurezza in vista di attività di volontariato che prevedono contatti diretti e regolari con minori o persone vulnerabili;

— espletare le procedure in materia di visti, acquisizione della cittadinanza e migrazione, comprese quelle di asilo; ed

— effettuare controlli in relazione ad appalti pubblici e concorsi pubblici.

Ciononostante, in casi specifici diversi da quelli in cui un cittadino di paese terzo chiede all'autorità centrale informazioni sul proprio casellario, o quando la richiesta è presentata per ottenere informazioni dal casellario giudiziale a norma dell'articolo 10, paragrafo 2, della direttiva 2011/93/UE, l'autorità che chiede informazioni sui casellari giudiziali può decidere che tale uso di ECRIS-TCN non è adeguato.

2. Uno Stato membro che decida, se previsto conformemente al diritto nazionale, di usare ECRIS-TCN per fini diversi da quelli indicati al paragrafo 1, allo scopo di ottenere informazioni su precedenti condanne tramite ECRIS, entro la data di entrata in funzione di cui all'articolo 35, paragrafo 4, o successivamente, notifica alla Commissione tali fini e le eventuali modifiche. La Commissione pubblica altresì tali notifiche nella *Gazzetta ufficiale dell'Unione europea* entro 30 giorni dal ricevimento della notifica.

3. Eurojust, Europol ed EPPO sono legittimati a interrogare ECRIS-TCN per individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo in conformità degli articoli da 14 a 18. Ciononostante, non inseriscono, rettificano o cancellano dati in ECRIS-TCN.

4. Ai fini di cui ai paragrafi 1, 2 e 3, le autorità competenti possono inoltre interrogare ECRIS-TCN per verificare se, con riguardo a un cittadino dell'Unione, uno o più Stati membri siano in possesso di informazioni sul casellario giudiziale di tale persona in quanto cittadino di paese terzo.

5. Quando interrogano ECRIS-TCN, le autorità competenti possono usare tutti o soltanto alcuni dei dati di cui all'articolo 5, paragrafo 1. L'insieme minimo di dati necessari per interrogare il sistema è specificato in un atto di esecuzione adottato in conformità dell'articolo 10, paragrafo 1, lettera g).

6. Le autorità competenti possono interrogare ECRIS-TCN anche usando le immagini del volto, sempreché tale funzionalità sia stata attuata a norma dell'articolo 6, paragrafo 2.

7. In caso di riscontro positivo, il sistema centrale trasmette automaticamente all'autorità competente le informazioni sugli Stati membri in possesso di informazioni sul casellario giudiziale del cittadino di paese terzo, insieme con i numeri di riferimento associati ed eventuali corrispondenti informazioni sull'identità. Tali informazioni sull'identità sono utilizzate al solo scopo di verificare l'identità del cittadino di paese terzo interessato. Il risultato di un'interrogazione del sistema centrale può essere utilizzato al solo scopo di introdurre una richiesta ai sensi dell'articolo 6 della decisione quadro 2009/315/GAI o una richiesta di cui all'articolo 17, paragrafo 3, del presente regolamento.

8. In assenza di riscontro positivo, il sistema centrale ne informa automaticamente l'autorità competente.

CAPITOLO III

Conservazione e modifica dei dati

Articolo 8

Periodo di conservazione dei dati

1. Ciascuna registrazione record di dati è conservata nel sistema centrale fintanto che i dati relativi alla condanna o alle condanne pronunciate a carico dell'interessato sono conservati nel casellario giudiziale.

2. Allo scadere del periodo di conservazione di cui al paragrafo 1, l'autorità centrale dello Stato membro di condanna cancella dal sistema centrale la registrazione di dati, incluse le impronte digitali e le immagini del volto. La cancellazione avviene automaticamente, se possibile, e in ogni caso non oltre un mese dalla scadenza del periodo di conservazione.

Articolo 9

Modifica e cancellazione dei dati

1. Gli Stati membri possono modificare o cancellare i dati da essi inseriti in ECRIS-TCN.

2. Qualsiasi modifica delle informazioni nei casellari giudiziali che hanno generato una registrazione di dati ai sensi dell'articolo 5 include un'identica modifica, senza ingiustificato ritardo, da parte dello Stato membro di condanna, delle informazioni conservate in tale registrazione di dati nel sistema centrale.

3. Qualora abbia ragione di credere che i dati registrati nel sistema centrale sono inesatti o che sono stati trattati nel sistema centrale in violazione del presente regolamento, lo Stato membro di condanna:

a) avvia immediatamente una procedura di verifica dell'esattezza dei dati in questione o, se del caso, della liceità del proprio trattamento;

b) ove necessario, rettifica o cancella, senza ingiustificato ritardo, i dati dal sistema centrale.

4. Ove uno Stato membro diverso dallo Stato membro di condanna che ha introdotto i dati abbia ragione di credere che i dati registrati nel sistema centrale sono inesatti o che sono stati trattati nel sistema centrale in violazione del presente regolamento, esso contatta senza ingiustificato ritardo l'autorità centrale dello Stato membro di condanna.

Lo Stato membro di condanna:

a) avvia immediatamente una procedura di verifica dell'esattezza dei dati in questione o, se del caso, della liceità del loro trattamento;

b) se necessario, rettifica o cancella dal sistema centrale senza ingiustificato ritardo i dati in questione;

c) informa senza ingiustificato ritardo l'altro Stato membro dell'avvenuta rettifica o cancellazione dei dati, o dei motivi per cui i dati non sono stati rettificati né cancellati.

CAPITOLO V

Sviluppo, funzionamento e responsabilità

Articolo 10

Adozione di atti di esecuzione da parte della Commissione

1. La Commissione adotta gli atti di esecuzione necessari allo sviluppo tecnico e all'attuazione di ECRIS-TCN quanto prima, in particolare atti riguardanti:

a) le specifiche tecniche per il trattamento dei dati alfanumerici;

b) le specifiche tecniche per la qualità, la risoluzione e il trattamento delle impronte digitali;

c) le specifiche tecniche del software di interfaccia;

d) le specifiche tecniche per la qualità, la risoluzione e il trattamento delle immagini del volto per gli scopi e alle condizioni di cui all'articolo 6;

e) la qualità dei dati, compreso un meccanismo e procedure per lo svolgimento dei controlli di qualità;

f) l'inserimento dei dati conformemente all'articolo 5;

g) l'accesso e l'interrogazione di ECRIS-TCN conformemente all'articolo 7;

h) la modifica e la cancellazione dei dati conformemente agli articoli 8 e 9;

i) la conservazione dei registri e l'accesso a essi conformemente all'articolo 31;

j) il funzionamento dell'archivio centrale e le norme in materia di sicurezza e protezione dei dati applicabili all'archivio conformemente all'articolo 32;

k) l'elaborazione di statistiche conformemente all'articolo 32;

l) i requisiti di funzionamento e di disponibilità di ECRIS-TCN, tra cui specifiche e requisiti minimi sulle prestazioni biometriche di ECRIS-TCN, in particolare per quanto riguarda il tasso di falsa identificazione positiva e il tasso di falsa identificazione negativa richiesti.

2. Gli atti di esecuzione di cui al paragrafo 1 sono adottati secondo la procedura di esame di cui all'articolo 38, paragrafo 2.

Articolo 11

Sviluppo e gestione operativa di ECRIS-TCN

1. eu-Lisa è responsabile dello sviluppo dia ECRIS-TCN conformemente al principio della protezione dei dati fin dalla progettazione e per impostazione predefinita. eu-Lisa è altresì responsabile della gestione operativa di ECRIS-TCN. Lo sviluppo comporta l'elaborazione e l'applicazione delle specifiche tecniche, il collaudo e il coordinamento generale del progetto.

2. eu-Lisa è inoltre responsabile dello sviluppo ulteriore e della manutenzione dell'attuazione di riferimento ECRIS.

3. eu-LISA definisce la progettazione dell'architettura fisica di ECRIS-TCN, comprese le specifiche tecniche e l'evoluzione per quanto riguarda il sistema centrale, il punto di accesso centrale nazionale e il software d'interfaccia. La progettazione è adottata dal suo consiglio di amministrazione, previo parere favorevole della Commissione.

4. eu-LISA sviluppa e realizza ECRIS-TCN quanto prima dopo l'entrata in vigore del presente regolamento e dopo l'adozione da parte della Commissione degli atti di esecuzione di cui all'articolo 10.

5. Prima della fase di progettazione e di sviluppo di ECRIS-TCN, il consiglio di amministrazione di eu-LISA istituisce un consiglio di gestione del programma composto di dieci membri.

Il consiglio di gestione del programma è costituito da otto membri nominati dal consiglio di amministrazione, dal presidente del gruppo consultivo di cui all'articolo 39 e da un membro nominato dalla Commissione. I membri nominati dal consiglio di amministrazione sono eletti soltanto tra gli Stati membri che sono pienamente vincolati in base al diritto dell'Unione dagli strumenti legislativi che disciplinano ECRIS e che parteciperanno a ECRIS-TCN. Il consiglio di amministrazione garantisce che i membri da esso nominati al consiglio di gestione del programma dispongano dell'esperienza e delle competenze necessarie in termini di sviluppo e gestione di sistemi IT a sostegno delle autorità giudiziarie e delle autorità incaricate dei casellari giudiziali.

eu-LISA partecipa ai lavori del consiglio di gestione del programma. A tal fine, rappresentanti di eu-LISA prendono parte alle riunioni del consiglio di gestione del programma allo scopo di riferire in merito ai lavori relativi alla progettazione e allo sviluppo di ECRIS-TCN e a eventuali altri lavori e attività correlati.

Il consiglio di gestione del programma si riunisce almeno una volta a trimestre e più spesso se necessario. Esso garantisce l'adeguata gestione della fase di progettazione e di sviluppo di ECRIS-TCN e la coerenza tra il progetto centrale e i progetti nazionali dell'ECRIS-TCN, e con il software nazionale di attuazione di ECRIS. Il consiglio di gestione del programma presenta regolarmente e se possibile mensilmente, relazioni scritte al consiglio di amministrazione di eu-LISA sui progressi del progetto. Il consiglio di gestione del programma non ha potere decisionale né mandato di rappresentare i membri del consiglio di amministrazione.

6. Il consiglio di gestione del programma stabilisce il suo regolamento interno, che comprende in particolare disposizioni concernenti:

a) la presidenza;

b) i luoghi di riunione;

c) la preparazione delle riunioni;

d) l'ammissione di esperti alle riunioni;

e) i piani di comunicazione atti a garantire che siano tenuti completamente informati i membri non partecipanti del consiglio di amministrazione.

7. La presidenza del consiglio di gestione del programma è esercitata da uno Stato membro che è pienamente vincolato, conformemente al diritto dell'Unione, dagli strumenti legislativi che disciplinano ECRIS e dagli strumenti legislativi che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi IT su larga scala gestiti da eu-LISA.

8. Tutte le spese di viaggio e di soggiorno sostenute dai membri del consiglio di gestione del programma sono a carico di eu-LISA. L'articolo 10 del regolamento interno di eu-LISA si applica mutatis mutandis. Il segretariato del consiglio di gestione del programma è assicurato da eu-LISA.

9. In fase di progettazione e di sviluppo, il gruppo consultivo di cui all'articolo 39 è composto dei responsabili di progetto nazionali di ECRIS-TCN ed è presieduto da eu-LISA. In fase di progettazione e di sviluppo esso si riunisce regolarmente, se possibile almeno una volta al mese, fino all'entrata in funzione di ECRIS-TCN. Dopo ciascuna riunione, riferisce al consiglio di gestione del programma. Fornisce la consulenza tecnica a sostegno delle attività del consiglio di gestione del programma e monitora lo stato di preparazione degli Stati membri.

10. Al fine di garantire la riservatezza e l'integrità in qualsiasi momento dei dati conservati in ECRIS-TCN, eu-LISA, in cooperazione con gli Stati membri, prevede idonee misure tecniche e organizzative, tenendo conto dello stato dell'arte, del costo relativo all'attuazione e dei rischi associati al trattamento.

11. eu-LISA è responsabile dei seguenti compiti relativi all'infrastruttura di comunicazione di cui all'articolo 4, paragrafo 1, lettera d):

a) controllo;

b) sicurezza;

c) coordinamento delle relazioni tra gli Stati membri e il gestore dell'infrastruttura di comunicazione.

12. La Commissione è responsabile di tutti gli altri compiti connessi con l'infrastruttura di comunicazione di cui all'articolo 4, paragrafo 1, lettera d), in particolare:

a) compiti relativi all'esecuzione del bilancio;

b) acquisizione e rinnovo;

c) aspetti contrattuali.

13. eu-LISA sviluppa e mantiene un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati conservati in ECRIS-TCN e riferisce periodicamente agli Stati membri. eu-LISA riferisce periodicamente alla Commissione in merito ai problemi incontrati e agli Stati membri interessati.

14. La gestione operativa di ECRIS-TCN consiste nell'insieme dei compiti necessari per garantirne l'operatività in conformità del presente regolamento e comprende, in particolare, la manutenzione e gli adeguamenti tecnici necessari per garantire che ECRIS-TCN funzioni a un livello soddisfacente conformemente alle specifiche tecniche.

15. eu-LISA svolge compiti relativi alla formazione sull'uso tecnico di ECRIS-TCN e dell'attuazione di riferimento ECRIS.

16. Fatto salvo l'articolo 17 dello statuto dei funzionari dell'Unione europea di cui al regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio ([17]), eu-LISA applica a tutti i membri del proprio personale che devono lavorare con i dati registrati nel sistema centrale adeguate norme in materia di segreto professionale o altri doveri equivalenti di riservatezza. Questo obbligo vincola tale personale anche dopo che ha lasciato l'incarico o cessato di lavorare, ovvero portato a termine le sue attività.

Articolo 12

Responsabilità degli Stati membri

1. Ciascuno Stato membro è responsabile di quanto segue:

a) una connessione sicura tra le banche dati nazionali di casellari giudiziali e di impronte digitali e il punto di accesso centrale nazionale;

b) lo sviluppo, il funzionamento e la manutenzione della connessione di cui alla lettera a);

c) una connessione tra il sistema nazionale e l'attuazione di riferimento ECRIS;

([17]) GU L 56 del 4.3.1968, pag. 1.

d) la gestione e le modalità di accesso a ECRIS-TCN del personale debitamente autorizzato delle autorità centrali a norma del presente regolamento, nonché la compilazione e l'aggiornamento periodico di un elenco di tale personale con le qualifiche. di cui all'articolo 19, paragrafo 3, lettera g).

2. Ciascuno Stato membro provvede affinché il personale della sua autorità centrale con diritto di accesso a ECRIS-TCN riceva una formazione adeguata che riguardi, in particolare, le norme di sicurezza e di protezione dei dati e i diritti fondamentali applicabili, prima di autorizzarli a trattare dati conservati nel sistema centrale.

Articolo 13

Responsabilità per l'uso dei dati

1. Conformemente alle norme applicabili dell'Unione in materia di protezione dei dati, ciascuno Stato membro garantisce che i dati registrati in ECRIS-TCN siano trattati lecitamente e, in particolare, che:

a) soltanto il personale debitamente autorizzato abbia accesso ai dati per assolvere i propri compiti;

b) i dati siano raccolti lecitamente e nel pieno rispetto della dignità umana e dei diritti fondamentali del cittadino di paese terzo;

c) i dati siano inseriti lecitamente in ECRIS-TCN;

d) i dati inseriti in ECRIS-TCN siano esatti e aggiornati.

2. eu-LISA garantisce che ECRIS-TCN sia gestito conformemente al presente regolamento, agli atti delegati di cui all'articolo 6, paragrafo 2, e agli atti di esecuzione di cui all'articolo 10, nonché conformemente al regolamento (UE) 2018/1725. In particolare eu-LISA adotta le misure necessarie per garantire la sicurezza del sistema centrale e dell'infrastruttura di comunicazione di cui all'articolo 4, paragrafo 1, lettera d), fatte salve le responsabilità di ciascuno Stato membro.

3. eu-LISA informa il Parlamento europeo, il Consiglio, la Commissione e il garante europeo della protezione dei dati il più presto possibile delle misure adottate in conformità del paragrafo 2 in vista dell'entrata in funzione dia ECRIS-TCN.

4. La Commissione mette a disposizione degli Stati membri e del pubblico, mantenendo regolarmente aggiornato il sito web, le informazioni di cui al paragrafo 3.

Articolo 14

Accesso di Eurojust, Europol ed EPPO

1. Eurojust ha accesso diretto a ECRIS-TCN ai fini dell'attuazione dell'articolo 17 e dello svolgimento dei suoi compiti di cui all'articolo 2 del regolamento (UE) 2018/1727, per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi.

2. Europol ha accesso diretto a ECRIS-TCN ai fini dello svolgimento dei suoi compiti di cui all'articolo 4, paragrafo 1, lettere e) e h), del regolamento (UE) 2016/794, per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi.

3. EPPO ha accesso diretto a ECRIS-TCN ai fini dello svolgimento dei suoi compiti di cui all'articolo 4 del regolamento (UE) 2017/1939, per individuare lo Stato membro o gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi.

4. A seguito di riscontro positivo che indichi gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di un cittadino di paese terzo, Eurojust, Europol ed EPPO possono contattare le autorità nazionali di tali Stati membri per chiedere le informazioni sui casellari giudiziali nel modo previsto nei rispettivi strumenti giuridici costitutivi.

Articolo 15

Accesso da parte di personale autorizzato di Eurojust, Europol ed EPPO

Eurojust, Europol ed EPPO sono responsabili della gestione e delle modalità di accesso a ECRIS-TCN da parte del personale debitamente autorizzato a norma del presente regolamento e della compilazione e dell'aggiornamento periodico di un elenco di tale personale con le relative qualifiche.

Articolo 16

Responsabilità di Eurojust, Europol ed EPPO

Eurojust, Europol ed EPPO:

a) stabiliscono i mezzi tecnici per connettersi a ECRIS-TCN e sono responsabili del mantenimento della connessione;

b) forniscono una formazione adeguata che riguardi, in particolare, le norme di sicurezza e di protezione dei dati e i diritti fondamentali applicabili, ai membri del loro personale con diritto di accesso a ECRIS-TCN prima di autorizzarli a trattare dati conservati nel sistema centrale;

c) garantiscono che i dati personali che trattano a norma del presente regolamento siano protetti conformemente alle norme applicabili in materia di protezione dei dati.

Articolo 17

Punto di contatto per i paesi terzi e le organizzazioni internazionali

1. I paesi terzi e le organizzazioni internazionali possono, ai fini di un procedimento penale, indirizzare a Eurojust richieste di informazioni su quali Stati membri, se del caso, siano in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo. A tale scopo utilizzano il formulario standard che figura nell'allegato del presente regolamento.

2. Quando riceve una richiesta a norma del paragrafo 1, Eurojust usa ECRIS-TCN per individuare gli eventuali Stati membri in possesso di informazioni sul casellario giudiziale del cittadino di paese terzo interessato.

3. In caso di riscontro positivo, Eurojust chiede agli Stati membri in possesso di informazioni sul casellario giudiziale del cittadino di paese terzo interessato se acconsentono a che Eurojust informi il paese terzo o l'organizzazione internazionale del nome dello Stato membro interessato. Se tale Stato membro fornisce il proprio consenso, Eurojust comunica al paese terzo o all'organizzazione internazionale il nome di detto Stato membro e le modalità di introduzione di una richiesta di estratti del casellario giudiziale presso gli Stati membri in questione, secondo le procedure applicabili.

4. In assenza di riscontro positivo o qualora non sia in grado di fornire una risposta, conformemente al paragrafo 3, alle richieste che le sono state presentate ai sensi del presente articolo, Eurojust informa il paese terzo o l'organizzazione internazionale in questione di aver completato la procedura, senza precisare se le informazioni sul casellario giudiziale della persona interessata siano in possesso di uno Stato membro.

Articolo 18

Comunicazione di informazioni a un paese terzo, a un'organizzazione internazionale o a un soggetto privato

Né Eurojust, né Europol, né EPPO, né alcuna delle autorità centrali trasmette a paesi terzi, organizzazioni internazionali o soggetti privati, o mette a loro disposizione, informazioni ottenute tramite ECRIS-TCN relative a un cittadino di paese terzo. Il presente articolo fa salvo l'articolo 17, paragrafo 3.

Articolo 19

Sicurezza dei dati

1. eu-LISA adotta le misure necessarie per garantire la sicurezza di ECRIS-TCN, fatte salve le responsabilità di ciascuno Stato membro, tenuto conto delle misure di sicurezza di cui al paragrafo 3.

2. Per quanto riguarda il funzionamento di ECRIS-TCN, eu-LISA adotta le misure necessarie per conseguire gli obiettivi enunciati al paragrafo 3, compresa l'adozione di un piano di sicurezza e di un piano di continuità operativa e di ripristino in caso di disastro, e garantire che i sistemi installati possano, in caso di interruzione, essere ripristinati.

3. Gli Stati membri garantiscono la sicurezza dei dati prima e durante la trasmissione al punto di accesso centrale nazionale e il ricevimento dallo stesso. In particolare ciascuno Stato membro:

a) protegge fisicamente i dati, tra l'altro mediante l'elaborazione di piani di emergenza per la protezione delle infrastrutture;

b) nega alle persone non autorizzate l'accesso alle strutture nazionali nelle quali lo Stato membro effettua operazioni connesse a ECRIS-TCN;

c) impedisce che supporti di dati possano essere letti, copiati, modificati o asportati senza autorizzazione;

d) impedisce l'inserimento di dati senza autorizzazione e l'ispezione, la modifica o la cancellazione senza autorizzazione di dati personali memorizzati;

e) impedisce il trattamento dei dati in ECRIS-TCN senza autorizzazione e la modifica o la cancellazione senza autorizzazione dei dati trattati nel sistema ECRIS-TCN;

f) garantisce che le persone autorizzate ad accedere a ECRIS-TCN abbiano accesso soltanto ai dati previsti dalla loro autorizzazione di accesso, ricorrendo all'identificativo utente individuale e utilizzando esclusivamente modalità di accesso riservato;

g) garantisce che tutte le autorità con diritto di accedere a ECRIS-TCN creino profili che descrivono le funzioni e le responsabilità delle persone autorizzate ad accedere ai dati e a inserire, rettificare, cancellare, consultare e interrogare i dati, e mettano senza ingiustificato ritardo tali profili a disposizione delle autorità nazionali di controllo, su richiesta di queste ultime;

h) garantisce la possibilità di verificare e stabilire a quali organi, organismi e agenzie dell'Unione possano essere trasmessi dati personali mediante apparecchiature di comunicazione dei dati;

i) garantisce che sia possibile verificare e stabilire quali dati sono stati trattati in ECRIS-TCN, quando, da chi e per quale finalità;

j) impedisce, in particolare mediante tecniche appropriate di cifratura, che all'atto della trasmissione di dati personali da ECRIS-TCN o verso di esso, oppure durante il trasporto dei supporti di dati, tali dati personali possano essere letti, copiati, modificati o cancellati senza autorizzazione;

k) controlla l'efficacia delle misure di sicurezza di cui al presente paragrafo e adotta le necessarie misure di carattere organizzativo relative alla verifica e alla verifica interna per garantire l'osservanza del presente regolamento.

4. eu-LISA e gli Stati membri cooperano al fine di garantire un approccio coerente alla sicurezza dei dati sulla base di una procedura di gestione del rischio di sicurezza che includa l'intero ECRIS-TCN.

Articolo 20

Responsabilità

1. Le persone o gli Stati membri che hanno subito un danno materiale o non materiale in conseguenza di un trattamento illecito di dati o di qualsiasi altro atto incompatibile con il presente regolamento hanno diritto di ottenere un risarcimento:

a) dallo Stato membro responsabile del danno; o

b) nel caso in cui eu-LISA non abbia soddisfatto i propri obblighi di cui al presente regolamento o al regolamento (UE) 2018/1725.

Lo Stato membro responsabile del danno o eu-LISA sono rispettivamente esonerati in tutto o in parte da tale responsabilità se provano che l'evento dannoso non è loro imputabile.

2. Ogni Stato membro, Eurojust, Europol o EPPO sono rispettivamente responsabili per i danni causati a ECRIS-TCN in caso di inosservanza da parte loro degli obblighi derivanti dal presente regolamento, tranne nel caso e nei limiti in cui eu-LISA o un altro Stato membro che partecipa a ECRIS-TCN abbia omesso di adottare misure ragionevolmente idonee a evitare i danni o a minimizzarne gli effetti.

3. Le azioni proposte nei confronti di uno Stato membro per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono disciplinate dal diritto dello Stato membro convenuto. Le azioni proposte nei confronti di eu-LISA, Eurojust, Europol ed EPPO per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono disciplinate dai loro rispettivi strumenti giuridici costitutivi.

Articolo 21

Verifica interna

Gli Stati membri provvedono affinché ogni autorità centrale adotti le misure necessarie per conformarsi al presente regolamento e cooperi, se necessario, con le autorità di controllo.

Articolo 22

Sanzioni

L'uso improprio dei dati inseriti in ECRIS-TCN è oggetto di sanzioni o di misure disciplinari effettive, proporzionate e dissuasive, secondo il diritto nazionale o dell'Unione.

CAPITOLO V

Diritti e controllo sulla protezione dei dati

Articolo 23

Titolare del trattamento e responsabile del trattamento

1. Per quanto riguarda il trattamento dei dati personali effettuato dall'autorità centrale di uno Stato membro a norma del presente regolamento, titolare del trattamento ai sensi delle norme applicabili dell'Unione in materia di protezione dei dati è l'autorità centrale di tale Stato membro.

2. Per quanto riguarda l'inserimento dei dati personali nel sistema centrale da parte degli Stati membri, eu-LISA è responsabile del trattamento ai sensi del regolamento (UE) 2018/1725.

Articolo 24

Finalità del trattamento dei dati personali

1. I dati inseriti nel sistema centrale sono trattati al solo fine di individuare gli Stati membri in possesso di informazioni sui casellari giudiziali su cittadini di paesi terzi.

2. Ad eccezione del personale debitamente autorizzato di Eurojust, Europol ed EPPO, che ha accesso a ECRIS-TCN ai fini del presente regolamento, l'accesso a ECRIS-TCN è riservato esclusivamente al personale debitamente autorizzato delle autorità centrali. L'accesso è limitato a quanto necessario all'assolvimento dei compiti, conformemente al fine di cui al paragrafo 1, e a quanto necessario e proporzionato agli obiettivi perseguiti.

Articolo 25

Diritto di accesso, rettifica, cancellazione e limitazione del trattamento

1. Le richieste dei cittadini di paesi terzi relative ai diritti di accesso ai dati personali, di rettifica o cancellazione nonché di limitazione del trattamento, sanciti dalle norme applicabili dell'Unione in materia di protezione dei dati, possono essere presentate all'autorità centrale di ogni Stato membro.

2. Qualora la richiesta sia presentata a uno Stato membro diverso da quello di condanna, lo Stato membro al quale è stata presentata la richiesta la trasmette allo Stato membro di condanna senza ingiustificato ritardo e comunque entro di dieci giorni lavorativi dal suo ricevimento. Non appena riceve la richiesta, lo Stato membro di condanna:

a) avvia immediatamente una procedura di verifica dell'esattezza dei dati interessati o della liceità del loro trattamento in ECRIS-TCN; e

b) risponde allo Stato membro che ha presentato la domanda senza ingiustificato ritardo.

3. Qualora emerga che i dati registrati in ECRIS-TCN sono inesatti o sono stati trattati illecitamente, lo Stato membro di condanna provvede a rettificarli o a cancellarli conformemente all'articolo 9. Lo Stato membro di condanna o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta, conferma per iscritto e senza ingiustificato ritardo all'interessato di aver provveduto a rettificare o cancellare i dati che lo riguardano. Lo Stato membro di condanna comunica inoltre senza ingiustificato ritardo quali misure sono state adottate a qualsiasi altro Stato membro che abbia ricevuto informazioni relative alla condanna ottenute da una interrogazione di ECRIS-TCN.

4. Qualora non ritenga che i dati registrati in ECRIS-TCN siano di fatto inesatti o siano stati registrati illecitamente, lo Stato membro di condanna adotta una decisione amministrativa o giudiziaria con la quale illustra per iscritto all'interessato la ragione per cui non intende rettificare o cancellare i dati che lo riguardano. Tali casi possono, se del caso, essere comunicati all'autorità nazionale di controllo.

5. Lo Stato membro che ha adottato la decisione ai sensi del paragrafo 4 fornisce inoltre all'interessato informazioni in merito alla procedura da seguire qualora egli non ritenga accettabile la motivazione fornita ai sensi del paragrafo 4. Tali informazioni comprendono le informazioni sulle modalità per avviare un'azione o un reclamo presso le autorità competenti o le autorità giurisdizionali competenti di tale Stato membro e su qualunque tipo di assistenza, compresa quella delle autorità nazionali di controllo, disponibile in conformità del diritto nazionale di tale Stato membro.

6. Qualsiasi richiesta presentata a norma del paragrafo 1 contiene le informazioni necessarie per identificare l'interessato. Tali informazioni sono utilizzate unicamente per consentire l'esercizio dei diritti di cui al paragrafo 1 e sono cancellate subito dopo.

7. Se si applica il paragrafo 2, l'autorità centrale a cui è stata presentata la richiesta conserva una registrazione scritta della presentazione di tale richiesta e di come e a quale autorità è stata trasmessa. Su richiesta dell'autorità di controllo nazionale, l'autorità centrale mette senza ritardo tale registrazione a disposizione di tale autorità nazionale di controllo. L'autorità centrale e l'autorità nazionale di controllo cancellano tali registrazioni tre anni dopo la loro creazione.

Articolo 26

Cooperazione volta a garantire il rispetto dei diritti relativi alla protezione dei dati

1. Le autorità centrali cooperano per garantire il rispetto dei diritti sanciti dall'articolo 25.

2. In ciascuno Stato membro l'autorità nazionale di controllo fornisce, su richiesta, informazioni agli interessati sull'esercizio del diritto di rettifica o cancellazione dei dati che li riguardano, ai sensi delle norme applicabili dell'Unione in materia di protezione dei dati.

3. Ai fini del presente articolo, l'autorità nazionale di controllo dello Stato membro che ha trasmesso i dati e l'autorità di controllo nazionali dello Stato membro alle quali è stata presentata la richiesta cooperano per raggiungere tali obiettivi.

Articolo 27

Mezzi di ricorso

Chiunque ha il diritto di presentare un reclamo e il diritto a un ricorso giuridico nello Stato membro di condanna che abbia negato il diritto di cui all'articolo 25, di ottenere l'accesso ovvero la rettifica o la cancellazione dei dati che lo riguardano, in conformità del diritto nazionale o dell'Unione.

Articolo 28

Vigilanza da parte delle autorità nazionali di controllo

1. Ciascuno Stato membro assicura che le autorità nazionali di controllo designate in conformità delle norme applicabili dell'Unione in materia di protezione dei dati verifichino la liceità del trattamento dei dati personali di cui agli articoli 5 e 6 effettuato dallo Stato membro in questione, nonché il loro trasferimento al e da ECRIS-TCN.

2. L'autorità nazionale di controllo provvede affinché, almeno ogni tre anni dalla data dell'entrata in funzione di ECRIS-TCN, sia svolto un audit dei trattamenti di dati nelle banche dati nazionali di casellari giudiziali e di impronte digitali relativamente allo scambio di dati tra tali sistemi e ECRIS-TCN, conformemente ai pertinenti principi internazionali di audit.

3. Gli Stati membri provvedono affinché le loro autorità nazionali di controllo dispongano delle risorse sufficienti per assolvere i compiti a esse affidati dal presente regolamento.

4. Ciascuno Stato membro comunica qualsiasi informazione richiesta dalle autorità nazionali di controllo e, in particolare, fornisce loro informazioni sulle attività svolte conformemente agli articoli 12, 13 e 19. Ciascuno Stato membro consente alle proprie autorità nazionali di controllo di consultare le registrazioni conformemente all'articoli 25, paragrafo 7, e l'accesso ai propri registri conformemente all'articolo 31, paragrafo 6, e consente loro l'accesso in qualsiasi momento a tutti i suoi locali utilizzati per ECRIS-TCN.

Articolo 29

Vigilanza da parte del garante europeo della protezione dei dati

1. Il garante europeo della protezione dei dati verifica che le attività di trattamento dei dati personali da parte di eu-LISA concernenti ECRIS-TCN siano effettuate in conformità del presente regolamento.

2. Il garante europeo della protezione dei dati provvede affinché, almeno ogni tre anni, sia svolto un audit delle attività di trattamento dei dati personali effettuate da eu-LISA, conformemente ai pertinenti principi internazionali di audit. Una relazione su tale audit è trasmessa al Parlamento europeo, al Consiglio, alla Commissione, a eu-LISA e alle autorità di controllo. A eu-LISA è data la possibilità di presentare osservazioni prima dell'adozione della relazione.

3. eu-LISA fornisce al garante europeo della protezione dei dati le informazioni da questo richieste, gli permette di consultare tutti i documenti e i registri di cui all'articolo 31 e di avere accesso, in qualsiasi momento, a tutti i suoi locali.

Articolo 30

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

È assicurato il controllo coordinato di ECRIS-TCN a norma dell'articolo 62 del regolamento (UE) 2018/1725.

Articolo 31

Registri

1. eu-LISA e le autorità competenti provvedono, nei limiti delle responsabilità rispettive, affinché tutti i trattamenti di dati in ECRIS-TCN siano registrati conformemente al paragrafo 2 al fine di verificare l'ammissibilità delle richieste e monitorare l'integrità e la sicurezza dei dati e la liceità del trattamento dei dati, nonché a fini di verifica interna.

2. Il registro indica:

a) lo scopo della richiesta di accesso ai dati di ECRIS-TCN;

b) i dati trasmessi di cui all'articolo 5;

c) il riferimento dell'archivio nazionale;

d) la data e l'ora esatta del trattamento;

e) i dati usati per l'interrogazione;

f) l'identificazione del funzionario che ha effettuato la consultazione.

3. Il registro delle consultazioni e delle comunicazioni consente di stabilire la motivazione di tali operazioni.

4. I registri sono usati solo ai fini della verifica della liceità del trattamento dei dati e per garantire l'integrità e la sicurezza dei dati. Soltanto i registri che non contengono dati personali possono essere usati ai fini della verifica e della valutazione di cui all'articolo 36. Tali registri sono protetti dall'accesso non autorizzato con misure adeguate e sono cancellati dopo tre anni, sempreché non siano stati richiesti per procedure di verifica già avviate.

5. Su richiesta, eu-LISA mette a disposizione delle autorità centrali, senza ingiustificato ritardo, i registri dei propri trattamenti.

6. Le autorità nazionali di controllo competenti a verificare l'ammissibilità della richiesta e la liceità del trattamento dei dati, l'integrità e la sicurezza dei dati, hanno accesso ai registri, su loro richiesta per l'adempimento delle loro funzioni. Su richiesta, le autorità centrali mettono a disposizione delle autorità nazionali di controllo competenti, senza ingiustificato ritardo, i registri dei propri trattamenti.

CAPITOLO VI

Disposizioni finali

Articolo 32

Uso dei dati per l'elaborazione di relazioni e statistiche

1. Il personale debitamente autorizzato di eu-LISA, delle autorità competenti e della Commissione è abilitato a consultare i dati trattati in ECRIS-TCN unicamente per elaborare relazioni e statistiche e senza che sia possibile l'identificazione individuale.

2. Ai fini del paragrafo 1, eu-LISA crea, attua e ospita nei suoi siti tecnici un archivio centrale contenente i dati di cui al paragrafo 1 che, senza rendere possibile l'identificazione individuale, consentono di ottenere relazioni e dati statistici personalizzabili. L'accesso all'archivio centrale è garantito mediante un accesso sicuro con controllo dell'accesso e specifici profili di utente unicamente ai fini dell'elaborazione di relazioni e statistiche.

3. Le procedure poste in essere da eu-LISA per monitorare il funzionamento di ECRIS-TCN di cui all'articolo 36 e l'attuazione di riferimento ECRIS comprendono la possibilità di produrre statistiche periodiche a fini di monitoraggio.

Ogni mese eu-LISA trasmette alla Commissione statistiche relative alla registrazione, alla conservazione e allo scambio delle informazioni estratte dai casellari giudiziali tramite ECRIS-TCN e l'attuazione di riferimento ECRIS. eu-LISA garantisce che non è possibile identificare i dati individuali sulla base di tali statistiche. Su richiesta della Commissione, eu-LISA le fornisce statistiche su aspetti specifici connessi all'attuazione del presente regolamento.

4. Gli Stati membri forniscono a eu-LISA le statistiche necessarie per adempiere agli obblighi di cui al presente articolo. Essi forniscono alla Commissione statistiche relative al numero di cittadini di paesi terzi condannati e al numero di condanne di cittadini di paesi terzi sul loro territorio.

Articolo 33

Spese

1. Le spese sostenute per l'istituzione e il funzionamento del sistema centrale, dell'infrastruttura di comunicazione di cui all'articolo 4, paragrafo 1, lettera d), del software di interfaccia e dell'attuazione di riferimento ECRIS sono a carico del bilancio generale dell'Unione.

2. Le spese di connessione di Eurojust, Europol ed EPPO a ECRIS-TCN sono a carico del loro rispettivo bilancio.

3. Altre spese sono a carico degli Stati membri, in particolare quelle sostenute per la connessione dei registri nazionali di casellari giudiziali, delle banche dati di impronte digitali e delle autorità centrali a ECRIS-TCN, e le spese di hosting dell'attuazione di riferimento ECRIS.

Articolo 34

Comunicazioni

1. Ciascuno Stato membro comunica a eu-LISA l'autorità centrale o le autorità centrali che dispongono dell'accesso per inserire, rettificare, cancellare, consultare e interrogare i dati e la informa di ogni eventuale cambiamento al riguardo.

2. eu-LISA provvede alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea* e sul suo sito web dell'elenco delle autorità centrali comunicate dagli Stati membri. Non appena riceve la comunicazione di un cambiamento dell'autorità centrale di uno Stato membro, eu-LISA aggiorna l'elenco senza ingiustificato ritardo.

Articolo 35

Inserimento dei dati ed entrata in funzione

1. La Commissione determina la data a partire dalla quale gli Stati membri iniziano a inserire in ECRIS-TCN i dati di cui all'articolo 5 una volta che ha accertato che:

a) siano stati adottati gli atti di esecuzione pertinenti di cui all'articolo 10;

b) gli Stati membri abbiano convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere a ECRIS-TCN i dati di cui all'articolo 5 e le abbiano comunicate alla Commissione;

c) eu-LISA abbia effettuato un collaudo generale di ECRIS-TCN, in cooperazione con gli Stati membri, utilizzando dati di prova anonimi.

2. Quando la Commissione ha determinato la data di inizio dell'inserimento dei dati conformemente al paragrafo 1, la comunica agli Stati membri. Entro un periodo di due mesi a decorrere da tale data gli Stati membri inseriscono in ECRIS-TCN i dati di cui all'articolo 5, tenendo conto dell'articolo 41, paragrafo 2.

3. Alla fine del periodo di cui al paragrafo 2, eu-LISA esegue un collaudo finale di ECRIS-TCN, in cooperazione con gli Stati membri.

4. Quando il collaudo di cui al paragrafo 3 è stato completato con successo ed eu-LISA ritiene che ECRIS-TCN sia pronto a entrare in funzione, essa lo comunica alla Commissione. La Commissione informa il Parlamento europeo e il Consiglio dell'esito del collaudo e decide la data a partire dalla quale ECRIS-TCN entra in funzione.

5. La decisione della Commissione sulla data di entrata in funzione di ECRIS-TCN, di cui al paragrafo 4, è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

6. Gli Stati membri iniziano a utilizzare ECRIS-TCN a decorrere dalla data stabilita dalla Commissione ai sensi del paragrafo 4.

7. Nell'adottare le decisioni di cui al presente articolo, la Commissione può fissare date diverse per l'inserimento in ECRIS-TCN dei dati alfanumerici e dei dati relativi alle impronte digitali di cui all'articolo 5, nonché per l'entrata in funzione relativamente a tali diverse categorie di dati.

Articolo 36

Monitoraggio e valutazione

1. eu-LISA provvede affinché siano istituite procedure per monitorare lo sviluppo di ECRIS-TCN rispetto agli obiettivi relativi alla programmazione e ai costi, nonché a monitorare il funzionamento di ECRIS-TCN e dell'attuazione di riferimento ECRIS rispetto agli obiettivi concernenti i risultati tecnici, il rapporto costi/benefici, la sicurezza e la qualità del servizio.

2. Ai fini del monitoraggio del funzionamento di ECRIS-TCN e della sua manutenzione tecnica, eu-LISA ha accesso alle informazioni necessarie riguardanti i trattamenti dei dati effettuati in ECRIS-TCN e nell'attuazione di riferimento ECRIS.

3. Entro il 10 dicembre 2019 e successivamente ogni sei mesi durante la fase di progettazione e sviluppo, eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sullo sviluppo di ECRIS-TCN e dell'attuazione di riferimento ECRIS.

4. La relazione di cui al paragrafo 3 include una panoramica dei costi attuali e dell'evoluzione del progetto, una valutazione dell'impatto finanziario, nonché informazioni su eventuali problemi tecnici e rischi suscettibili di ripercuotersi sui costi complessivi di ECRIS-TCN a carico del bilancio generale dell'Unione in conformità dell'articolo 33.

5. In caso di importante ritardo nel processo di sviluppo, eu-LISA informa il Parlamento europeo e il Consiglio quanto prima dei motivi di tale ritardo, nonché del relativo impatto finanziario e sul calendario.

6. Una volta che lo sviluppo di ECRIS-TCN e dell'attuazione di riferimento ECRIS è completato, eu-LISA presenta una relazione al Parlamento europeo e al Consiglio che illustra in che modo gli obiettivi sono stati conseguiti, in particolare per quanto riguarda la programmazione e i costi, giustificando eventuali scostamenti.

7. Nel caso di un aggiornamento tecnico di ECRIS-TCN, che potrebbe comportare costi elevati, eu-LISA informa il Parlamento europeo e il Consiglio.

8. Due anni dopo l'entrata in funzione di ECRIS-TCN e successivamente ogni anno, eu-LISA presenta alla Commissione una relazione sul funzionamento tecnico di ECRIS-TCN e dell'attuazione di riferimento ECRIS, compresa la loro sicurezza, basata in particolare sulle statistiche relative al funzionamento e all'uso di ECRIS-TCN e allo scambio, tramite l'attuazione di riferimento ECRIS, delle informazioni estratte dai casellari giudiziali.

9. Quattro anni dopo l'entrata in funzione di ECRIS-TCN e successivamente ogni quattro anni, la Commissione effettua una valutazione globale di ECRIS-TCN e dell'attuazione di riferimento ECRIS. La relazione di valutazione globale elaborata su questa base comprende una valutazione dell'applicazione del presente regolamento e un'analisi concernente i risultati conseguiti in relazione agli obiettivi fissati e l'incidenza sui diritti fondamentali. Sono incluse inoltre una valutazione della perdurante validità dei principi di base del funzionamento di ECRIS-TCN, una valutazione dell'adeguatezza dell'uso dei dati biometrici ai fini del funzionamento di ECRIS-TCN, della sicurezza di ECRIS-TCN e delle eventuali implicazioni in termini di sicurezza per le future attività. La valutazione comprende le necessarie raccomandazioni. La Commissione trasmette la relazione al Parlamento europeo, al Consiglio, al garante europeo della protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali.

10. Inoltre, la prima valutazione globale di cui al paragrafo 9 include una valutazione dei seguenti aspetti:

a) la misura in cui, sulla base dei pertinenti dati statistici e delle ulteriori informazioni fornite dagli Stati membri, l'inclusione in ECRIS-TCN di informazioni sull'identità di cittadini dell'Unione che possiedono anche la cittadinanza di un paese terzo ha contribuito al conseguimento degli obiettivi del presente regolamento;

b) la possibilità, per alcuni Stati membri, di continuare a usare il software nazionale di attuazione ECRIS, ai sensi dell'articolo 4;

c) l'inserimento dei dati relativi alle impronte digitali in ECRIS-TCN, in particolare l'applicazione dei criteri minimi di cui all'articolo 5, paragrafo 1, lettera b), punto ii);

d) l'incidenza di ECRIS e di ECRIS-TCN sulla protezione dei dati di carattere personale.

La valutazione può, se necessario, essere corredata di proposte legislative. Le valutazioni globali successive possono includere una valutazione di uno o di tutti questi aspetti.

11. Gli Stati membri, Eurojust, Europol ed EPPO comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 3, 8 e 9 conformemente agli indicatori quantitativi predefiniti dalla Commissione o da eu-LISA, o da entrambe. Tali informazioni non mettono a repentaglio i metodi di lavoro, né comprendono indicazioni sulle fonti, sui membri del personale o sulle indagini.

12. Ove opportuno, le autorità di controllo comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui al paragrafo 9 conformemente agli indicatori quantitativi predefiniti dalla Commissione o da eu-LISA, o da entrambe. Tali informazioni non mettono a repentaglio i metodi di lavoro, né comprendono indicazioni sulle fonti, sui membri del personale o sulle indagini.

13. eu-LISA comunica alla Commissione le informazioni necessarie per elaborare le valutazioni globali di cui al paragrafo 9.

Articolo 37

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 6, paragrafo 2, è conferito alla Commissione per un periodo indeterminato a decorrere dal 9 giugno 2019.

3. La delega di potere di cui all'articolo 6, paragrafo 2, 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 6, paragrafo 2, 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 38

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.

Qualora il comitato non esprima alcun parere, la Commissione non adotta il progetto di atto di esecuzione e si applica l'articolo 5, paragrafo 4, terzo comma, del regolamento (UE) n. 182/2011.

Articolo 39

Gruppo consultivo

eu-LISA istituisce un gruppo consultivo allo scopo di ottenere consulenza tecnica relativa a ECRIS-TCN e all'attuazione di riferimento ECRIS, in particolare nell'ambito della preparazione del programma di lavoro annuale e della relazione annuale di attività. In fase di progettazione e di sviluppo si applica l'articolo 11, paragrafo 9.

Articolo 40

Modifiche del regolamento (UE) 2018/1726

Il regolamento (UE) 2018/1726 è cosi modificato:

1) all'articolo 1, il paragrafo 4 è sostituito dal seguente:

«4. L'Agenzia è responsabile della preparazione, dello sviluppo o della gestione operativa del sistema di ingressi/uscite (EES), di DubliNet, del sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), di ECRIS-TCN e dell'attuazione di riferimento ECRIS.»;

2) è inserito l'articolo seguente:

«*Articolo 8 bis*

Compiti relativi a ECRIS-TCN e all'attuazione di riferimento ECRIS

Con riguardo a ECRIS-TCN e all'attuazione di riferimento ECRIS, l'Agenzia svolge:

a) i compiti attribuiti all'Agenzia conformemente al regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio (*);

b) i compiti relativi alla formazione sull'uso tecnico di ECRIS-TCN e dell'attuazione di riferimento ECRIS.

(*) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1).»;

3) all'articolo 14, il paragrafo 1 è sostituito dal seguente:

«1. L'Agenzia segue gli sviluppi della ricerca per la gestione operativa del SIS II, del VIS, di Eurodac, dell'EES, dell'ETIAS, di DubliNet, di ECRIS-TCN e di altri sistemi IT su larga scala di cui all'articolo 1, paragrafo 5.»;

4) all'articolo 19, il paragrafo 1 è così modificato:

a) la lettera ee) è sostituita dalla seguente:

«ee) adotta le relazioni sullo sviluppo dell'EES conformemente all'articolo 72, paragrafo 2, del regolamento (UE) 2017/2226, le relazioni sullo sviluppo dell'ETIAS conformemente all'articolo 92, paragrafo 2, del regolamento (UE) 2018/1240 e le relazioni sullo sviluppo di ECRIS-TCN e dell'attuazione di riferimento ECRIS conformemente all'articolo 36, paragrafo 3, del regolamento (UE) 2019/816;»;

b) la lettera ff) è sostituita dalla seguente:

«ff) adotta le relazioni sul funzionamento tecnico del SIS II in conformità, rispettivamente, dell'articolo 50, paragrafo 4, del regolamento (CE) n. 1987/2006 e dell'articolo 66, paragrafo 4, della decisione 2007/533/GAI, del VIS in conformità dell'articolo 50, paragrafo 3, del regolamento (CE) n. 767/2008 e dell'articolo 17, paragrafo 3, della decisione 2008/633/GAI, dell'EES in conformità dell'articolo 72, paragrafo 4, del regolamento (UE) 2017/2226, dell'ETIAS in conformità dell'articolo 92, paragrafo 4, del regolamento (UE) 2018/1240, e di ECRIS-TCN e dell'attuazione di riferimento ECRIS in conformità dell'articolo 36, paragrafo 8, del regolamento (UE) 2019/816;»;

c) la lettera hh) è sostituita dalla seguente:

«hh) adotta osservazioni formali sulle relazioni del Garante europeo della protezione dei dati relative ai controlli svolti conformemente all'articolo 45, paragrafo 2, del regolamento (CE) n. 1987/2006, all'articolo 42, paragrafo 2, del regolamento (CE) n. 767/2008 e all'articolo 31, paragrafo 2, del regolamento (UE) n. 603/2013, all'articolo 56, paragrafo 2, del regolamento (UE) 2017/2226 e all'articolo 67 del regolamento (UE) 2018/1240 e all'articolo 29, paragrafo 2, del regolamento (UE) 2019/816, e assicura adeguato seguito a tali controlli e audit;»;

d) è inserita la lettera seguente:

«ll bis) trasmette alla Commissione statistiche su ECRIS-TCN e sull'attuazione di riferimento ECRIS conformemente all'articolo 32, paragrafo 4, secondo comma, del regolamento (UE) 2019/816;»;

e) la lettera mm) è sostituita dalla seguente:

«mm) provvede alla pubblicazione annuale dell'elenco delle autorità competenti autorizzate a consultare direttamente i dati inseriti nel SIS II in conformità dell'articolo 31, paragrafo 8, del regolamento (CE) n. 1987/2006 e dell'articolo 46, paragrafo 8, della decisione 2007/533/GAI, e dell'elenco degli uffici dei sistemi nazionali del SIS II (uffici N.SIS II) e degli uffici SIRENE in conformità, rispettivamente, dell'articolo 7, paragrafo 3, del regolamento (CE) n. 1987/2006 e dell'articolo 7, paragrafo 3, della decisione 2007/533/GAI, nonché dell'elenco delle autorità competenti di cui all'articolo 65, paragrafo 2, del regolamento (UE) 2017/2226 e dell'elenco delle autorità competenti di cui all'articolo 87, paragrafo 2, del regolamento (UE) 2018/1240 e dell'elenco delle autorità centrali di cui all'articolo 34, paragrafo 2, del regolamento (UE) 2019/816;»;

5) all'articolo 22, paragrafo 4 è inserito il seguente comma dopo il terzo comma:

«Europol, Eurojust ed EPPO possono assistere alle riunioni del consiglio di amministrazione in qualità di osservatori quando sono all'ordine del giorno questioni concernenti ECRIS-TCN in relazione all'applicazione del regolamento (UE) 2019/816.»;

6) all'articolo 24, paragrafo 3, la lettera p) è sostituita dalla seguente:

«p) stabilire, fatto salvo l'articolo 17 dello statuto, le clausole di riservatezza per conformarsi all'articolo 17 del regolamento (CE) n. 1987/2006, all'articolo 17 della decisione 2007/533/GAI, all'articolo 26, paragrafo 9, del regolamento (CE) n. 767/2008, all'articolo 4, paragrafo 4, del regolamento (UE) n. 603/2013, all'articolo 37, paragrafo 4, del regolamento (UE) 2017/2226, all'articolo 74, paragrafo 2, del regolamento (UE) 2018/1240 e all'articolo 11, paragrafo 16, del regolamento (UE) 2019/816;»;

7) all'articolo 27, paragrafo 1, è inserito il seguente punto:

«d *bis*) gruppo consultivo di ECRIS-TCN;».

Articolo 41

Attuazione e disposizioni transitorie

1. Gli Stati membri adottano quanto prima le misure necessarie per conformarsi al presente regolamento in modo da garantire il corretto funzionamento di ECRIS-TCN.

2. Per le condanne pronunciate prima della data dell'avvio dell'inserimento dei dati ai sensi dell'articolo 35, paragrafo 1, le autorità centrali creano la registrazione di dati individuale nel sistema centrale come segue:

a) i dati alfanumerici che devono essere inseriti nel sistema centrale entro la fine del periodo di cui all'articolo 35, paragrafo 2;

b) i dati relativi alle impronte digitali che devono essere inseriti nel sistema centrale da ultimo entro due anni dall'entrata in funzione ai sensi dell'articolo 35, paragrafo 4.

Articolo 42

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione 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 Strasburgo, il 17 aprile 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ALLEGATO

FORMULARIO STANDARD PER LA RICHIESTA DI INFORMAZIONI AI SENSI DELL'ARTICOLO 17, PARAGRAFO 1, DEL REGOLAMENTO (UE) 2019/816 PER OTTENERE INFORMAZIONI SU QUALE STATO MEMBRO, SE ESISTE, È IN POSSESSO DI INFORMAZIONI SUL CASELLARIO GIUDIZIALE DI UN CITTADINO DI UN PAESE TERZO

Questo formulario, disponibile nelle 24 lingue ufficiali delle istituzioni dell'Unione sul sito www.eurojust.europa.eu, deve essere compilato in una delle lingue ufficiali e inviato all'indirizzo ECRIS-TCN@eurojust.europa.eu.di un cittadino di un paese terzo

Stato od organizzazione internazionale richiedente:

Nome dello Stato o dell'organizzazione internazionale:
Autorità che presenta la richiesta:
Rappresentata da (*nome della persona*):
Titolo:
Indirizzo:
Numero di telefono:
Indirizzo di posta elettronica:

Procedimenti penali oggetto della richiesta di informazioni:

Numero di riferimento nazionale:
Autorità competente:
Tipo di reati oggetto dell'indagine (*indicare i pertinenti articoli del codice penale*):
Altre informazioni pertinenti (*ad esempio urgenza della richiesta*):

Informazioni sull'identità della persona che ha la cittadinanza di un paese terzo e rispetto alla quale si ricercano informazioni sullo Stato membro di condanna:

Si prega di fornire il maggior numero di informazioni disponibili.

Cognome:
Nome o nomi:
Data di nascita:
Luogo di nascita (*città e paese*);
Cittadinanza (o cittadinanze):
Sesso:
Nomi precedenti, se del caso;
Nome dei genitori;
Numero d'identificazione:
Tipo e numero del documento (dei documenti) di identità della persona:
Autorità che ha rilasciato il o i documenti:
Eventuali pseudonimi o alias:
Fornire i dati relativi alle impronte digitali, se disponibili.

In caso di più persone, indicarle separatamente.

È possibile inserire altri soggetti utilizzando la finestra a discesa.

Luogo:	
Data:	

Firma e timbro (elettronici):

REGOLAMENTO (UE) 2019/817 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 20 maggio 2019

che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, paragrafo 2, l'articolo 74 e l'articolo 77, paragrafo 2, lettere a), b), d) ed e),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) Nella comunicazione del 6 aprile 2016 dal titolo «Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza», la Commissione ha sottolineato la necessità di migliorare l'architettura di gestione dei dati dell'Unione per la gestione delle frontiere e la sicurezza. La comunicazione ha dato il via a un processo mirante alla realizzazione dell'interoperabilità tra i sistemi di informazione dell'UE relativi alla sicurezza, alle frontiere e alla gestione della migrazione, allo scopo di colmare le carenze strutturali di tali sistemi che ostacolano il lavoro delle autorità nazionali, garantendo nel contempo che le guardie di frontiera, le autorità doganali, gli operatori di polizia e le autorità giudiziarie dispongano delle informazioni necessarie.

(2) Nella tabella di marcia per rafforzare lo scambio e la gestione di informazioni, comprese soluzioni di interoperabilità nel settore «Giustizia e affari interni» del 6 giugno 2016, il Consiglio ha individuato una serie di sfide giuridiche, tecniche e operative riguardanti l'interoperabilità dei sistemi di informazione dell'UE e ha sollecitato la ricerca di soluzioni.

(3) Nella risoluzione del 6 luglio 2016 sulle priorità strategiche per il programma di lavoro della Commissione per il 2017 ([3]), il Parlamento europeo ha chiesto proposte intese a migliorare e sviluppare i sistemi di informazione dell'UE esistenti, far fronte alla carenza di informazioni e progredire verso la loro interoperabilità, nonché proposte concernenti lo scambio obbligatorio di informazioni a livello dell'UE, assicurando nel contempo le necessarie garanzie in materia di protezione dei dati.

(4) Nelle conclusioni del 15 dicembre 2016 il Consiglio europeo ha sollecitato il conseguimento di ulteriori risultati sull'interoperabilità di sistemi di informazione e di banche dati dell'UE.

(5) Nella relazione finale dell'11 maggio 2017 il gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità ha concluso che era necessario e tecnicamente fattibile adoperarsi per giungere a soluzioni pratiche in materia di interoperabilità e che l'interoperabilità, in linea di massima, poteva offrire vantaggi operativi ed essere introdotta nel rispetto dei requisiti in materia di protezione dei dati.

([1]) GU C 283 del 10.8.2018, pag. 48.
([2]) Posizione del Parlamento europeo del 16 aprile 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 14 maggio 2019.
([3]) GU C 101 del 16.3.2018, pag. 116.

(6) Nella comunicazione del 16 maggio 2017 contenente la «Settima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza», la Commissione, in linea con quanto esposto nella comunicazione del 6 aprile 2016 e i risultati e le raccomandazioni del gruppo ad alto livello sui sistemi di informazione e l'interoperabilità, ha delineato un nuovo approccio alla gestione dei dati relativi alle frontiere, alla sicurezza e alla migrazione, in base al quale tutti i sistemi di informazione dell'UE per la gestione della sicurezza, delle frontiere e della migrazione dovevano essere interoperabili, in maniera tale da rispettare pienamente i diritti fondamentali.

(7) Nelle conclusioni del 9 giugno 2017 sulla via da seguire per migliorare lo scambio di informazioni e garantire l'interoperabilità dei sistemi d'informazione dell'UE, il Consiglio ha invitato la Commissione a portare avanti le soluzioni di interoperabilità proposte dal gruppo di esperti ad alto livello.

(8) Nelle conclusioni del 23 giugno 2017 il Consiglio europeo ha sottolineato la necessità di migliorare l'interoperabilità fra le banche dati e ha invitato la Commissione a elaborare quanto prima un progetto di normativa sulla base delle proposte formulate dal gruppo di esperti di alto livello sui sistemi di informazione e l'interoperabilità.

(9) Per migliorare l'efficacia e l'efficienza dei controlli alle frontiere esterne, contribuire a prevenire e contrastare l'immigrazione illegale e concorrere a garantire un alto livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, incluso il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri, migliorare l'attuazione della politica comune in materia di visti, assistere nell'esame delle domande di protezione internazionale, contribuire alla prevenzione, all'individuazione e all'indagine dei reati di terrorismo e di altri reati gravi, agevolare l'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati nel caso di una catastrofe naturale, incidente o attentato terroristico, al fine di preservare la fiducia dell'opinione pubblica nel sistema di migrazione e di asilo dell'Unione, nelle misure di sicurezza dell'Unione e nelle capacità di quest'ultima di gestire le frontiere esterne, è opportuno rendere interoperabili i sistemi di informazione dell'Unione, vale a dire il sistema di ingressi/uscite (EES), il sistema di informazione visti (VIS), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), l'Eurodac, il sistema d'informazione Schengen (SIS) e il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (ECRIS-TCN), affinché essi si integrino reciprocamente unitamente ai relativi dati, rispettando nel contempo i diritti fondamentali degli individui, in particolare il diritto alla protezione dei dati personali. A tal fine è opportuno istituire un portale di ricerca europeo (ESP), un servizio comune di confronto biometrico (BMS comune), un archivio comune di dati di identità (CIR) e un rilevatore di identità multiple (MID) che fungano da componenti dell'interoperabilità.

(10) L'interoperabilità dovrebbe consentire a tali sistemi di informazione dell'UE di integrarsi reciprocamente al fine di facilitare la corretta identificazione delle persone, tra cui le persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati, contribuire a contrastare la frode di identità, migliorare e uniformare i requisiti in materia di qualità dei dati dei rispettivi sistemi di informazione dell'UE, agevolare l'attuazione tecnica e operativa dei sistemi di informazione dell'UE da parte degli Stati membri, rafforzare la sicurezza e protezione dei dati che presiedono ai rispettivi sistemi di informazione dell'UE, razionalizzare l'accesso, a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, all'EES, al VIS, all'ETIAS e all'Eurodac a fini di contrasto e sostenere le finalità dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e di ECRIS-TCN.

(11) Le componenti dell'interoperabilità dovrebbero includere l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS ed ECRIS-TCN. Dovrebbero includere anche i dati Europol ma soltanto in modo tale da rendere possibile la consultazione dei dati Europol simultaneamente a quella dei suddetti sistemi di informazione dell'UE.

(12) Le componenti dell'interoperabilità dovrebbero trattare i dati personali delle persone i cui dati personali sono trattati nei sistemi di informazione dell'UE sottostanti e da Europol.

(13) È opportuno istituire l'ESP al fine di facilitare, dal punto di vista tecnico, l'accesso delle autorità degli Stati membri e delle agenzie dell'Unione, in modo rapido, continuato, efficace, sistematico e controllato, ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati dell'Organizzazione internazionale della polizia criminale (Interpol), nella misura in cui ciò è necessario per svolgere i loro compiti, conformemente ai rispettivi diritti di accesso. Inoltre è opportuno istituire l'ESP al fine di sostenere gli obiettivi dell'EES, del VIS, dell'ETIAS,

dell'Eurodac, del SIS, dell'ECRIS-TCN e dei dati Europol. Permettendo l'interrogazione parallela di tutti i sistemi di informazione dell'UE pertinenti, dei dati Europol e delle banche dati Interpol, l'ESP dovrebbe fungere da interfaccia unica o da mediatore di messaggi («message broker») per la consultazione di diversi sistemi centrali e per il recupero agevole delle informazioni necessarie, nel pieno rispetto dei requisiti concernenti il controllo degli accessi e la protezione dei dati dei sistemi sottostanti.

(14) L'ESP dovrebbe essere progettato in modo da garantire che quando interroga le banche dati Interpol i dati utilizzati da un utente ESP per avviare un'interrogazione non siano condivisi con i proprietari dei dati Interpol. L'ESP dovrebbe inoltre essere progettato in modo da garantire che le banche dati Interpol siano interrogate esclusivamente in conformità del diritto nazionale e dell'Unione applicabile.

(15) La banca dati sui documenti di viaggio rubati o smarriti (banca dati SLTD) dell'Interpol consente alle entità autorizzate, responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o altri reati gravi negli Stati membri, tra cui le autorità preposte ai servizi per l'immigrazione e al controllo delle frontiere, di accertare la validità di un documento di viaggio. L'ETIAS interroga la banca dati SLTD e la banca dati Interpol sui documenti di viaggio associati a segnalazioni (banca dati TDAWN) per valutare l'eventualità che una persona che sta facendo richiesta di autorizzazione ai viaggi possa, per esempio, migrare irregolarmente o rappresentare una minaccia per la sicurezza. L'ESP dovrebbe consentire le interrogazioni delle banche dati SLTD e TDAWN utilizzando i dati di identità o i dati del documento di viaggio di una persona fisica. Qualora i dati personali siano trasferiti dall'Unione a Interpol attraverso l'ESP, dovrebbero applicarsi le disposizioni in materia di trasferimenti internazionali di cui al capo V del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([4]), ovvero le disposizioni nazionali di recepimento del capo V della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([5]). Ciò dovrebbe lasciare impregiudicate le norme specifiche definite nella posizione comune 2005/69/GAI del Consiglio ([6]) e nella decisione 2007/533/GAI del Consiglio ([7]).

(16) L'ESP dovrebbe essere sviluppato e configurato in modo tale da consentire che tali interrogazioni siano effettuate soltanto attraverso l'uso di dati riguardanti persone o documenti di viaggio presenti in un sistema di informazione dell'UE, nei dati Europol o nelle banche dati Interpol.

(17) Per garantire l'utilizzo sistematico dei pertinenti sistemi di informazione dell'UE, l'ESP dovrebbe essere usato per interrogare il CIR, l'EES, il VIS, l' ETIAS, l'Eurodac e l'ECRIS-TCN. Un collegamento nazionale ai diversi sistemi di informazione dell'UE dovrebbe essere mantenuto, così da offrire la possibilità di ricorrere tecnicamente a una procedura sostitutiva. L'ESP dovrebbe inoltre essere utilizzato dalle agenzie dell'Unione per interrogare il SIS centrale conformemente ai rispettivi diritti di accesso e ai fini dell'espletamento dei loro compiti. Esso dovrebbe essere un mezzo supplementare per interrogare il SIS centrale, i dati Europol e le banche dati Interpol, integrando le interfacce dedicate esistenti.

(18) I dati biometrici quali le impronte digitali e le immagini del volto sono unici e di conseguenza molto più attendibili dei dati alfanumerici ai fini dell'identificazione di una persona. Il BMS comune dovrebbe essere uno strumento tecnico da utilizzare per rafforzare e agevolare il lavoro dei sistemi di informazione dell'UE pertinenti e delle altre componenti dell'interoperabilità. Lo scopo principale del BMS comune dovrebbe essere l'agevolazione dell'identificazione di una persona che è registrata in diverse banche dati utilizzando un'unica componente tecnologica per far corrisponderei dati biometrici di quella persona contenuti in diversi sistemi anziché più componenti. Il BMS comune dovrebbe contribuire alla sicurezza e offrire vantaggi in termini finanziari, operativi e di manutenzione. Tutti i sistemi automatizzati di identificazione dattiloscopica, inclusi quelli attualmente utilizzati per l'Eurodac, il VIS e il SIS, usano template biometrici costituiti da dati ricavati mediante estrazione di parametri di campioni biometrici effettivi. Il BMS comune dovrebbe riunire e conservare tutti i template biometrici – separati per logica in base al sistema di informazione di provenienza – in un unico luogo, facilitando il confronto trasversale ai vari sistemi mediante l'uso di template biometrici e permettendo economie di scala nello sviluppo e nella manutenzione dei sistemi centrali dell'UE.

([4]) 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).

([5]) 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).

([6]) Posizione comune 2005/69/GAI del Consiglio, del 24 gennaio 2005, sullo scambio con l'Interpol di alcuni dati (GU L 27 del 29.1.2005, pag. 61).

([7]) 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).

(19) I template biometrici conservati nel BMS comune dovrebbero essere costituiti da dati ricavati mediante estrazione di parametri di campioni biometrici effettivi, e ottenuti in modo tale che non sia possibile invertire il processo di estrazione. I template biometrici dovrebbero essere ottenuti da dati biometrici, ma non dovrebbe essere possibile ottenere gli stessi dati biometrici dai template biometrici. Poiché i dati sulle impronte palmari e i profili DNA sono conservati unicamente nel SIS e non possono essere utilizzati a fini di controlli incrociati con i dati contenuti in altri sistemi di informazione, conseguendo i principi di necessità e proporzionalità, il BMS comune non dovrebbe conservare i profili DNA o i template biometrici ottenuti dai dati sulle impronte palmari.

(20) I dati biometrici sono dati personali sensibili. Il presente regolamento dovrebbe stabilire le basi e le garanzie per il trattamento di tali dati allo scopo di identificare in modo univoco le persone interessate.

(21) I sistemi EES, VIS, ETIAS, Eurodac e ECRIS-TCN richiedono l'identificazione precisa delle persone di cui conservano i dati personali. Il CIR dovrebbe pertanto agevolare la corretta identificazione delle persone registrate in tali sistemi.

(22) I dati personali conservati in tali sistemi di informazione dell'UE possono riferirsi alle stesse persone, ma con identità differenti o incomplete. Gli Stati membri dispongono di modalità efficaci per identificare i propri cittadini o residenti permanenti iscritti nel loro territorio. L'interoperabilità tra i sistemi di informazione dell'UE dovrebbe contribuire alla corretta identificazione delle persone presenti in tali sistemi. Il CIR dovrebbe conservare i dati personali necessari per consentire un'identificazione più precisa delle persone i cui dati sono conservati in tali sistemi, compresi i dati di identità, i dati del documento di viaggio e i dati biometrici, a prescindere dal sistema nel quale tali dati sono stati inizialmente raccolti. Il CIR dovrebbe conservare solo i dati personali strettamente necessari per svolgere una verifica di identità accurata. I dati personali che vi sono registrati dovrebbero essere conservati per un arco di tempo non superiore a quanto strettamente necessario per il conseguimento delle finalità dei sistemi sottostanti e sono cancellati in modo automatico e concomitante alla loro cancellazione dai sistemi sottostanti, in base alla separazione logica.

(23) Una nuova operazione di trattamento consistente nel conservare questo tipo di dati nel CIR anziché in ciascun sistema separato è necessaria al fine di migliorare l'accuratezza dell'identificazione attraverso il confronto e l'abbinamento automatizzati dei dati. Il fatto che i dati di identità, i dati del documento di viaggio e biometrici siano conservati nel CIR non dovrebbe ostacolare in alcun modo il trattamento dei dati ai fini di EES, VIS, ETIAS, Eurodac o ECRIS-TCN, poiché il CIR dovrebbe essere una nuova componente comune di tali sistemi sottostanti.

(24) È necessario pertanto creare un fascicolo individuale nel CIR per ogni persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o in ECRIS-TCN ai fini di una corretta identificazione dei cittadini di paesi terzi all'interno dello spazio Schengen e quale supporto al funzionamento del MID, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. Il fascicolo individuale dovrebbe conservare tutte le informazioni relative all'identità connesse a una data persona in un unico luogo e renderle accessibili agli utenti finali debitamente autorizzati.

(25) Il CIR dovrebbe pertanto agevolare e semplificare l'accesso delle autorità responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o altri reati gravi ai sistemi di informazione dell'UE che non sono istituiti esclusivamente a fini di prevenzione, accertamento o indagine di reati gravi.

(26) Il CIR dovrebbe offrire un contenitore comune per i dati di identità, i dati del documento di viaggio e biometrici delle persone registrate nell'EES, nel VIS, nell'ETIAS, nell'Eurodac e nell' ECRIS-TCN. Dovrebbe rientrare nell'architettura tecnica di tali sistemi e fungere da componente comune tra di essi ai fini della conservazione e dell'interrogazione dei dati di identità, dei dati del documento di viaggio e biometrici che trattano.

(27) Tutte le registrazioni nel CIR dovrebbero essere separate logicamente mediante l'apposizione automatica, su ciascuna di esse, di un'etichetta che indichi il nome del sistema sottostante da cui provengono. Il sistema di controllo degli accessi del CIR dovrebbe utilizzare queste etichette per determinare se consentire o meno l'accesso alle registrazioni.

(28) Ove un'autorità di polizia di uno Stato membro non sia in grado di identificare una persona in ragione dell'assenza di un documento di viaggio o di un altro documento credibile che ne dimostri l'identità, ovvero ove sussistano dubbi quanto ai dati di identità forniti dall'interessato o all'autenticità del documento di viaggio

o all'identità del titolare, ovvero qualora l'interessato non sia in grado o rifiuti di cooperare, l'autorità in questione dovrebbe essere in grado di interrogare il CIR al fine di identificare la persona in oggetto. A tal fine, le autorità di polizia dovrebbero rilevare le impronte digitali utilizzando tecniche di scansione diretta (live-scan), a condizione che la procedura sia avviata in presenza di tale persona. Tali interrogazioni del CIR non dovrebbero essere autorizzate ai fini dell'identificazione di minori di età inferiore a 12 anni, a meno che ciò non sia nell'interesse superiore del minore.

(29) Se non si possono usare i dati biometrici dell'interessato o se un'interrogazione con tali dati non dà alcun esito, l'interrogazione dovrebbe essere effettuata con i dati di identità dell'interessato combinati con i dati del documento di viaggio. Se dall'interrogazione emerge che dati relativi all'interessato sono conservati nel CIR, le autorità dello Stato membro dovrebbero avere accesso al CIR per la consultazione dei dati di identità e dei dati del documento di viaggio di tale persona, senza che il CIR fornisca alcuna indicazione sul sistema di informazione dell'UE cui appartengono tali dati.

(30) Gli Stati membri dovrebbero adottare misure legislative nazionali per designare le autorità competenti a svolgere le verifiche di identità utilizzando il CIR e stabilendo le procedure, le condizioni e i criteri di queste verifiche, le quali dovrebbero rispettare il principio di proporzionalità. Dette misure, in particolare, dovrebbero conferire a tali autorità il potere di raccogliere dati biometrici della persona durante una verifica di identità effettuata in presenza di un loro rappresentante.

(31) Il presente regolamento dovrebbe altresì introdurre per le autorità designate dallo Stato membro responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o altri reati gravi e per Europol una nuova possibilità di accesso semplificato ad altri dati rispetto a quelli di identità o a quelli del documento di viaggio presenti nell'EES, nel VIS, nell'ETIAS o nell'Eurodac. Tali dati possono essere necessari, in casi specifici, a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, ove vi siano motivi ragionevoli per ritenere che la loro consultazione contribuirà alla prevenzione, all'accertamento o all'indagine dei reati di terrorismo o degli altri reati gravi, in particolare qualora sussista il sospetto che la persona sospettata, l'autore o la vittima di un reato di terrorismo o di un altro reato grave è una persona i cui dati sono conservati nell'EES, nel VIS, nell'ETIAS o nell'Eurodac.

(32) Il pieno accesso ai dati contenuti nell'EES, nel VIS, nell'ETIAS o nell'Eurodac che sia necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, diverso dall'accesso ai dati di identità o ai dati del documento di viaggio contenuti nel CIR, dovrebbe continuare a essere disciplinato dagli strumenti giuridici applicabili. Le autorità designate responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o altri reati gravi ed Europol non sanno in anticipo quale sistema di informazione dell'UE contenga dati sulle persone su cui devono compiere indagini. Ciò causa ritardi e inefficienze. Di conseguenza, l'utente finale autorizzato dall'autorità designata dovrebbe avere la facoltà di vedere in quale di tali sistemi di informazione dell'UE sono registrati i dati corrispondenti al risultato dell'interrogazione. Il sistema interessato verrebbe pertanto segnalato in esito alla verifica automatica della presenza di un riscontro positivo nel sistema (la cosiddetta funzione di segnalazione «match/no match»).

(33) In tale contesto, la risposta dal CIR non dovrebbe essere interpretata o utilizzata come motivo o ragione per trarre conclusioni o adottare misure riguardo a una persona, ma dovrebbe essere utilizzata soltanto per presentare una richiesta di accesso ai sistemi di informazione sottostanti dell'UE soggetta alle condizioni e alle procedure stabilite dai rispettivi strumenti giuridici che regolamentano tale accesso. Qualsiasi richiesta di accesso di questo genere dovrebbe essere soggetta al capo VII del presente regolamento e, laddove applicabile, al regolamento (UE) 2016/680, alla direttiva (UE) 2016/680 o al regolamento (UE) 2016/1725 del Parlamento europeo e del Consiglio ([8]).

(34) In linea di massima, se da un riscontro positivo emerge che i dati sono registrati nell'EES, nell'ETIAS o nel VIS o nell'Eurodac, è opportuno che le autorità designate o Europol richiedano il pieno accesso ad almeno uno dei sistemi di informazione dell'UE interessati. Ove, in via eccezionale, tale accesso integrale non sia richiesto, per esempio perché le autorità designate o Europol hanno già ottenuto i dati con altri mezzi o se il diritto nazionale non consente più di ottenere tali dati, è auspicabile registrare la motivazione della mancata richiesta di accesso.

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

(35) Le registrazioni delle interrogazioni nel CIR dovrebbero indicare lo scopo delle interrogazioni. Se l'interrogazione è stata effettuata utilizzando l'approccio di consultazione dei dati in due fasi, le registrazioni dovrebbero contenere un riferimento al fascicolo nazionale dell'indagine o del caso, indicando perciò che essa è stata avviata a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi.

(36) L'interrogazione del CIR da parte delle autorità designate e di Europol al fine di ottenere un riscontro che segnali la presenza o meno di dati nell'EES, nel VIS, nell'ETIAS o nell'Eurodac, richiede il trattamento automatizzato dei dati personali. La segnalazione del riscontro positivo non dovrebbe rivelare i dati personali dell'interessato, ma si limiterebbe a indicare che alcuni dei suoi dati sono conservati in uno dei sistemi. L'utente finale autorizzato non dovrebbe assumere alcuna decisione sfavorevole all'interessato basandosi unicamente sulla semplice segnalazione di un riscontro positivo. L'accesso dell'utente finale a tale segnalazione costituirà pertanto un'ingerenza molto limitata nel diritto alla protezione dei dati personali dell'interessato, consentendo allo stesso tempo alle autorità designate e a Europol di richiedere l'accesso ai dati personali in modo più efficace.

(37) È opportuno istituire il MID per sostenere il funzionamento del CIR, nonché gli obiettivi dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e dell' ECRIS-TCN. Per poter realizzare efficacemente i loro rispettivi obiettivi, questi sistemi di informazione dell'UE richiedono tutti un'identificazione precisa delle persone di cui conservano i dati personali.

(38) Ai fini di un migliore conseguimento degli obiettivi dei sistemi di informazione dell'UE, le autorità che li utilizzano dovrebbero poter effettuare verifiche sufficientemente affidabili dell'identità delle persone i cui dati sono conservati in sistemi diversi. L'insieme di dati di identità o di dati del documento di viaggio può essere inesatto, incompleto o fraudolento e, a oggi, non vi è alcun modo per rilevare dati di identità o dati del documento di viaggio fraudolenti, inesatti o incompleti mediante un confronto con i dati conservati in un altro sistema. Per rimediare a questa situazione è necessario dotarsi, a livello dell'Unione, di uno strumento tecnico che consenta un'identificazione precisa delle persone per tali scopi.

(39) Il MID dovrebbe creare e conservare i collegamenti tra i dati presenti nei vari sistemi di informazione dell'UE ai fini dell'individuazione di identità multiple, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. Il MID dovrebbe contenere solo i collegamenti tra i dati sulle persone fisiche presenti in più di un sistema di informazione dell'UE. I dati collegati dovrebbero essere limitati ai dati necessari per verificare se l'interessato è registrato in maniera giustificata o ingiustificata e con identità diverse in sistemi diversi, ovvero per chiarire che due persone aventi dati di identità simili possono non essere la stessa persona. Il trattamento dei dati mediante l'ESP e il BMS comune al fine di collegare i fascicoli individuali trasversalmente ai diversi sistemi dovrebbe limitarsi al minimo indispensabile e, pertanto, alla semplice rilevazione di un'identità multipla da condurre nel momento in cui sono aggiunti nuovi dati a uno dei sistemi che ha i dati raccolti nel CIR e nel SIS. Il MID dovrebbe prevedere misure di salvaguardia che tutelino le persone con identità multiple lecite da eventuali discriminazioni e decisioni sfavorevoli.

(40) Il presente regolamento prevede nuove operazioni di trattamento dei dati miranti a identificare in modo corretto le persone interessate. Ciò costituisce un'ingerenza nei loro diritti fondamentali tutelati dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Poiché l'attuazione efficace dei sistemi di informazione dell'UE dipende dalla corretta identificazione delle persone interessate, tale ingerenza è giustificata dagli stessi obiettivi per i quali ciascuno di questi sistemi è stato istituito, vale a dire: la gestione efficace delle frontiere dell'Unione, la sicurezza interna dell'Unione e l'attuazione efficace delle politiche dell'Unione in materia di asilo e di visti.

(41) Quando un'autorità nazionale o un'agenzia dell'Unione crea o carica nuove registrazioni, l'ESP e il BMS comune dovrebbero confrontare i dati riguardanti le persone contenuti nel CIR e nel SIS. Tale confronto dovrebbe essere automatizzato. Il CIR e il SIS dovrebbero utilizzare il BMS comune per individuare eventuali collegamenti sulla base dei dati biometrici. Dovrebbero utilizzare l'ESP per individuare eventuali collegamenti sulla base dei dati alfanumerici. Il CIR e il SIS dovrebbero essere in grado di individuare i dati identici o simili concernenti una persona conservati in più sistemi. In tal caso dovrebbe essere creato un collegamento che indichi che si tratta della stessa persona. Il CIR e il SIS dovrebbero essere configurati in modo tale da individuare i piccoli errori di ortografia o di traslitterazione, così da non creare ostacoli ingiustificati all'interessato.

(42) L'autorità nazionale o l'agenzia dell'Unione che ha registrato i dati nel sistema di informazione dell'UE pertinente dovrebbe confermare o modificare tali collegamenti. Tale autorità nazionale o agenzia dell'Unione dovrebbe avere accesso ai dati conservati nel CIR o nel SIS e nel MID ai fini della verifica manuale delle identità diverse.

(43) Una verifica manuale delle identità diverse dovrebbe competere all'autorità che ha creato o aggiornato i dati per i quali è emerso un riscontro positivo, che a sua volta ha dato luogo a un collegamento con i dati conservati in un altro sistema di informazione dell'UE. L'autorità responsabile della verifica manuale delle identità diverse dovrebbe accertare se esistano più identità che si riferiscono alla stessa persona in maniera giustificata o ingiustificata. Tale accertamento deve aver luogo, se possibile, in presenza della persona interessata, se del caso chiedendo ulteriori chiarimenti o informazioni. Dovrebbe essere effettuato senza indugio, nel rispetto dei requisiti giuridici riguardanti l'accuratezza delle informazioni ai sensi del diritto nazionale e dell'Unione. Soprattutto alle frontiere, la libertà di movimento delle persone interessate sarà soggetta a restrizioni per la durata della verifica, che non dovrebbe pertanto essere indefinita. L'esistenza di un collegamento giallo nel MID non dovrebbe costituire di per sé motivo di rifiuto dell'ingresso e qualsiasi decisione relativa all'autorizzazione o al rifiuto dell'ingresso dovrebbe essere adottata esclusivamente sulla base delle disposizioni applicabili del regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio ([9]).

(44) Per i collegamenti ottenuti attraverso il SIS relativamente a segnalazioni di persone ricercate per l'arresto a fini di consegna o di estradizione, di persone scomparse o vulnerabili, di persone ricercate per presenziare a un procedimento giudiziario o di persone da sottoporre a controllo discreto, a controllo di indagine o a controllo specifico, l'autorità responsabile della verifica manuale delle identità diverse dovrebbe essere l'ufficio SIRENE dello Stato membro che ha creato la segnalazione. Tali categorie di segnalazioni SIS sono sensibili e non dovrebbero essere necessariamente condivise con le autorità che inseriscono o aggiornano i dati collegati a essi in uno degli altri sistemi di informazione dell'UE. La creazione di un collegamento con i dati del SIS dovrebbe lasciare impregiudicate le azioni da intraprendere a norma dei regolamenti (UE) 2018/1860 ([10]), (UE) 2018/1861 ([11]) e (UE) 2018/1862 ([12]) del Parlamento europeo e del Consiglio.

(45) La creazione di tali collegamenti esige un atteggiamento trasparente nei confronti degli interessati. Al fine di agevolare l'attuazione delle necessarie garanzie in conformità delle norme applicabili dell'Unione in materia di protezione dei dati, le persone fisiche che, a seguito di una verifica manuale delle identità diverse, sono oggetto di un collegamento rosso o un collegamento bianco dovrebbero esserne informate per iscritto, fatte salve le limitazioni necessarie per proteggere la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non siano compromesse indagini nazionali. Tali persone fisiche dovrebbero ricevere un numero di identificazione unico che consenta loro di identificare l'autorità cui dovrebbero rivolgersi per esercitare i propri diritti.

(46) Qualora sia creato un collegamento giallo l'autorità responsabile della verifica manuale delle identità diverse dovrebbe avere accesso al MID. Qualora esista un collegamento rosso, le autorità degli Stati membri e le agenzie dell'Unione che hanno accesso ad almeno un sistema di informazione incluso nel CIR o al SIS dovrebbero avere accesso al MID. Il collegamento rosso dovrebbe indicare che una persona utilizza identità diverse in modo ingiustificato o che una persona utilizza l'identità di un'altra.

(47) Qualora esista un collegamento bianco o verde tra dati di due sistemi di informazione dell'UE, le autorità degli Stati membri e delle agenzie dell'Unione dovrebbero avere accesso al MID se l'autorità o agenzia interessata abbia accesso a entrambi i sistemi di informazione. Tale accesso dovrebbe essere accordato al solo scopo di consentire a tale autorità o agenzia di individuare potenziali casi di collegamento inesatto o in cui il trattamento dei dati nel MID, nel CIR e nel SIS è avvenuto in violazione del presente regolamento, e di adottare l'azione per correggere la situazione e aggiornare o cancellare il collegamento.

([9]) 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).

([10]) Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 312 del 7.12.2018, pag. 1).

([11]) Regolamento (UE) 2018/1861 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 (GU L 312 del 7.12.2018, pag. 14).

([12]) Regolamento (UE) 2018/1862 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 della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).

(48) L'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) dovrebbe istituire meccanismi automatizzati di controllo della qualità dei dati e indicatori comuni della qualità dei dati. eu-LISA dovrebbe essere responsabile dello sviluppo di una capacità centrale di monitoraggio della qualità dei dati e della redazione di relazioni periodiche di analisi dei dati, allo scopo di migliorare il controllo dell'attuazione dei sistemi di informazione dell'UE da parte degli Stati membri. Gli indicatori comuni sui dati dovrebbero includere norme minime di qualità per la conservazione dei dati nei sistemi di informazione dell'UE o nelle componenti dell'interoperabilità. Tali norme di qualità dei dati dovrebbero avere come obiettivo quello di consentire ai sistemi di informazione dell'UE e alle componenti dell'interoperabilità di individuare automaticamente i dati inviati che sono palesemente errati o incoerenti, affinché lo Stato membro da cui provengono sia in grado di verificarli e di provvedere a tutte le misure correttive necessarie.

(49) La Commissione dovrebbe valutare le relazioni di eu-LISA riguardanti la qualità e, se del caso, dovrebbe rivolgere raccomandazioni agli Stati membri. Gli Stati membri dovrebbero elaborare un piano d'azione che illustri le misure correttive volte a colmare le eventuali carenze nella qualità dei dati e dovrebbero riferire regolarmente in merito ai progressi compiuti.

(50) Il formato universale dei messaggi (UMF) dovrebbe fungere quale standard per lo scambio strutturato delle informazioni a livello transfrontaliero tra i sistemi di informazione, le autorità e/o le organizzazioni del settore Giustizia e affari interni. Per le informazioni scambiate abitualmente, l'UMF dovrebbe definire un lessico comune e strutture logiche che facilitino l'interoperabilità permettendo la creazione e la lettura del contenuto dello scambio in modo coerente e semanticamente equivalente.

(51) L'attuazione dello standard UMF può essere contemplata per il VIS, il SIS e qualunque altro modello esistente per lo scambio di informazioni o sistema di informazione transfrontaliero, nuovo o esistente, del settore Giustizia e affari interni sviluppato dagli Stati membri.

(52) È opportuno istituire un archivio centrale di relazioni e statistiche (CRRS) al fine di generare dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati, in conformità degli strumenti giuridici applicabili. eu-LISA dovrebbe istituire, attuare e ospitare il CRRS nei suoi siti tecnici. Dovrebbe contenere dati statistici anonimi provenienti dai sistemi di informazione dell'UE, dal CIR, dal MID e dal BMS comune. I dati contenuti nel CRRS non dovrebbero permettere l'identificazione delle persone fisiche. eu-LISA dovrebbe anonimizzare automaticamente i dati e dovrebbe registrare nel CRRS i dati così anonimizzati. Il processo di anonimizzazione dovrebbe essere automatizzato e il personale di eu-LISA non dovrebbe essere autorizzato in alcun modo ad accedere direttamente ai dati personali conservati nei sistemi di informazione dell'UE o nelle componenti dell'interoperabilità.

(53) Il regolamento (UE) 2016/679 si applica al trattamento dei dati personali finalizzato all'interoperabilità ai sensi del presente regolamento da parte delle autorità nazionali, a meno che tale trattamento non sia effettuato dalle autorità designate o dai punti di accesso centrale degli Stati membri a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi.

(54) Qualora il trattamento di dati personali da parte degli Stati membri finalizzato all'interoperabilità ai sensi del presente regolamento sia effettuato dalle autorità competenti a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, si applica la direttiva (UE) 2016/680.

(55) Il regolamento (UE) 2016/679, il regolamento (UE) 2018/1725 o, se del caso, la direttiva (UE) 2016/680 si applicano a qualsiasi trasferimento di dati personali verso paesi terzi o organizzazioni internazionali effettuati ai sensi del presente regolamento. Fatti salvi i motivi di trasferimento a norma del capo V del regolamento (UE) 2016/679 o, se del caso, della direttiva (UE) 2016/680, le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento dovrebbero essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro.

(56) Le disposizioni specifiche sulla protezione dei dati di cui ai regolamenti (UE) 2017/2226 ([13]), (CE) n. 767/2008 ([14]), (UE) 2018/1240 del Parlamento europeo e del Consiglio ([15]) e (UE) 2018/1861 dovrebbero applicarsi al trattamento dei dati personali nei sistemi disciplinati da tali regolamenti.

(57) Il regolamento (UE) 2018/1725 si applica al trattamento dei dati personali da parte di eu-LISA e di altre istituzioni e organi dell'Unione nell'assolvimento delle loro responsabilità a norma del presente regolamento, fatto salvo il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ([16]), che si applica al trattamento dei dati personali da parte di Europol.

(58) Le autorità di controllo di cui al regolamento (UE) 2016/679 o alla direttiva (UE) 2016/680 dovrebbero verificare la legittimità del trattamento dei dati personali da parte degli Stati membri. Il garante europeo della protezione dei dati dovrebbe sorvegliare le attività delle istituzioni e degli organismi dell'Unione connesse al trattamento dei dati personali. Il garante europeo della protezione dei dati e le autorità di controllo dovrebbero collaborare nel sorvegliare il trattamento dei dati personali da parte delle componenti dell'interoperabilità. Affinché il garante europeo della protezione dei dati assolva i compiti che gli sono affidati dal presente regolamento, sono necessarie risorse sufficienti, in particolare risorse umane e finanziarie.

(59) 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 ([17]) e ha espresso un parere il 16 aprile 2018 ([18]).

(60) Il gruppo di lavoro «Articolo 29» sulla protezione dei dati ha fornito un parere l'11 aprile 2018.

(61) Sia gli Stati membri che eu-LISA dovrebbero dotarsi di piani di sicurezza che agevolino l'adempimento degli obblighi in tal senso e dovrebbero collaborare per poter risolvere le questioni relative alla sicurezza. eu-LISA dovrebbe inoltre assicurare l'uso continuo dei più recenti sviluppi tecnologici, al fine di garantire l'integrità dei dati nel contesto dello sviluppo, della progettazione e della gestione delle componenti dell'interoperabilità. Gli obblighi di eu-LISA a tal riguardo dovrebbero includere l'adozione delle misure necessarie per impedire l'accesso delle persone non autorizzate, per esempio il personale dei fornitori esterni di servizi, ai dati personali trattati attraverso le componenti dell'interoperabilità. In sede di aggiudicazione dei contratti per la prestazione di servizi, gli Stati membri ed eu-LISA dovrebbero considerare tutte le misure necessarie per garantire la conformità alle disposizioni legislative e regolamentari in materia di protezione dei dati personali e della vita privata delle persone fisiche o per salvaguardare interessi essenziali di sicurezza, conformemente al regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio ([19]) e alle convenzioni internazionali applicabili. eu-LISA dovrebbe applicare i principi della tutela della vita privata fin dalla progettazione e per impostazione predefinita durante la fase di sviluppo delle componenti dell'interoperabilità.

(62) L'attuazione delle componenti dell'interoperabilità di cui al presente regolamento inciderà sul modo in cui saranno eseguite le verifiche ai valichi di frontiera. Gli effetti che ne deriveranno saranno il risultato dell'applicazione combinata delle vigenti norme del regolamento (UE) 2016/399 e delle norme sull'interoperabilità di cui al presente regolamento.

(63) Come conseguenza di questa applicazione combinata di norme, l'ESP dovrebbe rappresentare il punto di accesso principale per la consultazione sistematica obbligatoria delle banche dati prevista dal regolamento (UE) 2016/399 nei confronti delle persone ai valichi di frontiera. Per valutare se una persona soddisfa o meno le condizioni d'ingresso definite nel regolamento (UE) 2016/399, le guardie di frontiera dovrebbero inoltre tener conto dei dati

([13]) Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011 (GU L 327 del 9.12.2017, pag. 20).

([14]) Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS) (GU L 218 del 13.8.2008, pag. 60).

([15]) Regolamento (EU) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (EU) 2016/1624 e (UE) 2017/2226 (GU L 236 del 19.9.2018, pag. 1).

([16]) 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).

([17]) 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).

([18]) GU C 233 del 4.7.2018, pag. 12.

([19]) Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012 (GU L 193 del 30.7.2018, pag. 1).

di identità o dei dati del documento di viaggio che nel MID hanno portato alla classificazione di un collegamento con il colore rosso. Tuttavia, poiché la presenza di un collegamento rosso non dovrebbe costituire di per sé una giustificazione per respingere una persona, i motivi di respingimento attualmente previsti dal regolamento (UE) 2016/399 non dovrebbero essere modificati.

(64) Per rendere esplicite queste precisazioni sarebbe opportuno aggiornare il manuale pratico per le guardie di frontiera.

(65) Qualora un'interrogazione del MID, tramite l'ESP, generi un collegamento giallo o rilevi un collegamento rosso, la guardia di frontiera dovrebbe consultare il CIR o il SIS, o entrambi, al fine di valutare le informazioni sulla persona sottoposta a verifica, verificarne manualmente i dati sulla diversa identità e, se del caso, modificare il colore del collegamento.

(66) A sostegno dell'elaborazione di statistiche e relazioni, è necessario concedere al personale autorizzato delle autorità competenti, delle istituzioni dell'Unione e delle agenzie di cui al presente regolamento l'accesso alla consultazione di taluni dati relativi a determinate componenti dell'interoperabilità, senza permettere l'identificazione delle persone interessate.

(67) Per consentire alle autorità dello Stato membro e alle agenzie dell'Unione di adeguarsi ai nuovi requisiti relativi all'uso dell'ESP è necessario prevedere un periodo transitorio. Analogamente, dovrebbero essere stabilite misure transitorie per l'entrata in funzione del MID, al fine di consentirne un funzionamento coerente e ottimale.

(68) Poiché l'obiettivo del presente regolamento, vale a dire l'istituzione di un quadro per l'interoperabilità tra i sistemi di informazione dell'UE, non può essere conseguito in misura sufficiente dagli Stati membri ma può, a motivo della portata e degli effetti dell'azione in questione, essere conseguito 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 tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(69) L'importo rimanente della dotazione di bilancio destinata alle «frontiere intelligenti» di cui al regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio ([20]) dovrebbe essere riassegnato al presente regolamento, ai sensi dell'articolo 5, paragrafo 5, lettera b), del regolamento (UE) n. 515/2014, per coprire i costi di sviluppo delle componenti dell'interoperabilità.

(70) Al fine di integrare alcuni aspetti tecnici dettagliati del presente regolamento, è opportuno delegare alla Commissione il potere di adottare atti in conformità dell'articolo 290 del trattato sul funzionamento dell'Unione europea (TFUE) che riguardino:

— la proroga del periodo transitorio per l'uso dell'ESP;

— la proroga del periodo transitorio per l'uso del MID dall'unità centrale ETIAS;

— le procedure per stabilire i casi in cui i dati di identità possono essere considerati identici o simili;

— le norme relative al funzionamento del CRRS, comprese le garanzie specifiche per il trattamento dei dati personali e le norme di sicurezza applicabili all'archivio; e

— le norme dettagliate concernenti il funzionamento del portale web.

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 ([21]). In particolare, al fine di garantire una partecipazione paritaria alla preparazione degli atti delegati, è opportuno che il Parlamento europeo e il Consiglio ricevano l'intera documentazione contemporaneamente agli esperti degli Stati membri e che i loro esperti abbiano sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti.

(71) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione per la fissazione delle date a partire dalle quali l'ESP, il BMS comune, il CIR, il MID e il CRRS entrano in funzione.

([20]) 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).

([21]) GU L 123 del 12.5.2016, pag. 1.

(72) È altresì opportuno attribuire alla Commissione competenze di esecuzione per l'adozione di norme dettagliate riguardanti: le modalità tecniche dei profili per gli utenti dell'ESP; le specifiche della soluzione tecnica per facilitare l'interrogazione dei sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol mediante l'ESP e il formato delle risposte dell'ESP; le norme tecniche per la creazione di collegamenti nel MID tra dati di diversi sistemi di informazione dell'UE; il contenuto e la presentazione del modulo per informare l'interessato in caso di creazione di un collegamento rosso; i requisiti di prestazione e monitoraggio delle prestazioni del BMS comune; i meccanismi, le procedure e gli indicatori automatizzati di controllo della qualità dei dati; lo sviluppo dello standard UMF; la procedura di cooperazione in caso di incidenti di sicurezza; e le specifiche della soluzione tecnica per la gestione delle richieste di accesso degli utenti da parte degli Stati membri. È opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([22]).

(73) Poiché le componenti dell'interoperabilità comporteranno il trattamento di quantità significative di dati personali sensibili, è importante che le persone i cui dati sono trattati tramite dette componenti possano esercitare effettivamente i loro diritti in quanto interessati come prescritto a norma del regolamento (UE) 2016/679, della direttiva (UE) 2016/680 e del regolamento (UE) 2018/1725. Gli interessati dovrebbero disporre di un portale web che li agevoli nell'esercizio dei diritti di accesso, rettifica, cancellazione e limitazione del trattamento dei loro dati personali. eu-LISA dovrebbe istituire e gestire tale portale web.

(74) Uno dei principi fondamentali della protezione dei dati personali è la minimizzazione dei dati: ai sensi dell'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679, il trattamento dei dati personali deve essere adeguato, pertinente e limitato al minimo necessario rispetto alle finalità perseguite. Per questo motivo, le componenti dell'interoperabilità non dovrebbero prevedere la conservazione di nuovi dati personali, a eccezione dei collegamenti che saranno conservati nel MID e che costituiscono il minimo indispensabile ai fini del presente regolamento.

(75) È opportuno che il presente regolamento preveda disposizioni chiare in materia di responsabilità e il diritto al risarcimento per danni causati dal trattamento illecito di dati personali e da qualsiasi altro atto incompatibile con esso. Tali disposizioni dovrebbero far fatti salvi il diritto al risarcimento e la responsabilità da parte del titolare del trattamento o del responsabile del trattamento ai sensi del regolamento (UE) 2016/679, della direttiva (UE) 2016/680, e del regolamento (UE) 2018/1725. eu-LISA dovrebbe rispondere dei danni da essa causati in quanto responsabile del trattamento se non ha adempiuto gli obblighi del presente regolamento specificatamente gravanti su di essa o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni dello Stato membro titolare del trattamento.

(76) Il presente regolamento non pregiudica l'applicazione della direttiva 2004/38/CE del Parlamento europeo e del Consiglio ([23]).

(77) 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, nella misura in cui le sue disposizioni riguardano il SIS disciplinato dal regolamento (UE) n. 2018/1862, si basa sull'*acquis* di Schengen, la Danimarca decide, ai sensi dell'articolo 4 di tale protocollo, entro sei mesi dalla decisione del Consiglio sul presente regolamento, se intende recepirlo nel proprio diritto interno.

(78) 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 ([24]); il Regno Unito non partecipa pertanto alla sua adozione, non è da esso vincolato né è soggetto alla sua applicazione.

(79) 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 ([25]); l'Irlanda non partecipa pertanto alla sua adozione, non è da esso vincolata né è soggetta alla sua applicazione.

([22]) 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).

([23]) 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 e 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).

([24]) 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).

([25]) 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).

(80) 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 ([26]), uno sviluppo delle disposizioni dell'*acquis* di Schengen che rientrano nel settore di cui all'articolo 1, lettere A, B, C e G, della decisione 1999/437/CE del Consiglio ([27]).

(81) 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 ([28]), uno sviluppo delle disposizioni dell'*acquis* di Schengen che rientrano nel settore di cui all'articolo 1, lettere A, B, C e G, della decisione 1999/437/CE del Consiglio, in combinato disposto con l'articolo 3 della decisione 2008/146/CE del Consiglio ([29]).

(82) Per quanto riguarda il Liechtenstein, il presente regolamento costituisce, ai sensi del protocollo sottoscritto 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 ([30]), uno sviluppo delle disposizioni dell'*acquis* di Schengen che rientrano nel settore di cui all'articolo 1, lettere A, B, C e G, della decisione 1999/437/CE del Consiglio, in combinato disposto con l'articolo 3 della decisione 2011/350/UE del Consiglio ([31]).

(83) Il presente regolamento rispetta i diritti fondamentali e osserva i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea e dovrebbe essere applicato conformemente a tali diritti e principi.

(84) Per integrare il presente regolamento nel quadro giuridico esistente, è opportuno modificare di conseguenza i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 e le decisioni 2004/512/CE ([32]) e 2008/633/GAI del Consiglio ([33]),

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

Disposizioni generali

Articolo 1

Oggetto

1. Il presente regolamento, unitamente al regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio ([34]), istituisce un quadro per garantire l'interoperabilità tra il sistema di ingressi/uscite (EES), il sistema di informazione visti (VIS), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), l'Eurodac, il sistema d'informazione Schengen (SIS) e il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (ECRIS-TCN).

([26]) GU L 176 del 10.7.1999, pag. 36.

([27]) 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).

([28]) GU L 53 del 27.2.2008, pag. 52.

([29]) 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).

([30]) GU L 160 del 18.6.2011, pag. 21.

([31]) 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).

([32]) Decisione 2004/512/CE del Consiglio, dell'8 giugno 2004, che istituisce il sistema di informazione visti (VIS) (GU L 213 del 15.6.2004, pag. 5).

([33]) Decisione 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi (GU L 218 del 13.8.2008, pag. 129).

([34]) Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'Unione nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (Cfr. pag. 85 della presente Gazzetta ufficiale).

2. Il quadro consta delle seguenti componenti dell'interoperabilità:

a) un portale di ricerca europeo (ESP);

b) un servizio comune di confronto biometrico (BMS comune);

c) un archivio comune di dati di identità (CIR);

d) un rilevatore di identità multiple (MID).

3. Il presente regolamento fissa le disposizioni relative ai requisiti di qualità dei dati, al formato universale dei messaggi (UMF) e a un archivio centrale di relazioni e statistiche (CRRS), e stabilisce le responsabilità degli Stati membri e dell'Agenzia europea per la gestione operativa di sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) per quanto riguarda la progettazione, lo sviluppo e il funzionamento delle componenti dell'interoperabilità.

4. Il presente regolamento adatta le procedure e le condizioni per l'accesso delle autorità designate degli Stati membri e dell'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) all'EES, al VIS, all'ETIAS e all'Eurodac a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi.

5. Il presente regolamento stabilisce inoltre un quadro per il controllo delle identità delle persone e per l'identificazione delle persone.

Articolo 2

Obiettivi

1. Garantendo l'interoperabilità, il presente regolamento persegue i seguenti obiettivi:

a) migliorare l'efficacia e l'efficienza delle verifiche di frontiera alle frontiere esterne;

b) contribuire a prevenire e combattere l'immigrazione illegale;

c) contribuire ad 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;

d) migliorare l'attuazione della politica comune in materia di visti;

e) assistere nell'esame delle domande di protezione internazionale;

f) contribuire alla prevenzione, all'accertamento e all'indagine di reati di terrorismo o altri reati gravi;

g) facilitare l'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati nel caso di una catastrofe naturale, incidente o attentato terroristico.

2. Gli obiettivi di cui al paragrafo 1 sono realizzati:

a) garantendo la corretta identificazione delle persone;

b) contribuendo a combattere la frode di identità;

c) migliorando la qualità dei dati e armonizzando i requisiti di qualità per i dati conservati nei sistemi di informazione dell'UE, nel rispetto dei requisiti concernenti il trattamento dei dati previsti dagli strumenti giuridici dei singoli sistemi e delle norme e dei principi in materia di protezione dei dati;

d) agevolando e sostenendo gli Stati membri nell'attuazione tecnica e operativa dei sistemi di informazione dell'UE;

e) rafforzando, semplificando e rendendo più uniformi le condizioni di sicurezza e protezione dei dati che disciplinano i diversi sistemi di informazione dell'UE, facendo salve la protezione speciale e le garanzie previste per talune categorie di dati;

f) semplificando le condizioni di accesso delle autorità designate all'EES, al VIS, all'ETIAS e all'Eurodac, garantendo al contempo condizioni necessarie e proporzionate per tale accesso;

g) sostenendo le finalità dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e dell'ECRIS-TCN.

Articolo 3

Ambito di applicazione

1. Il presente regolamento si applica all'EES, al VIS, all'ETIAS e al SIS.

2. Il presente regolamento si applica alle persone i cui dati personali possono essere trattati nei sistemi di informazione dell'UE di cui al paragrafo 1 del presente articolo e i cui dati sono raccolti ai fini di cui agli articoli 1 e 2 del regolamento (CE) n. 767/2008, all'articolo 1 del regolamento (UE) 2017/2226, agli articoli 1 e 4 del regolamento (UE) 2018/1240, all'articolo 1 del regolamento (UE) 2018/1860 e all'articolo 1 del regolamento (UE) 2018/1861.

Articolo 4

Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

1) «frontiere esterne»: le frontiere esterne quali definite all'articolo 2, punto 2), del regolamento (UE) 2016/399;

2) «verifiche di frontiera»: le verifiche di frontiera quali definite all'articolo 2, punto 11), del regolamento (UE) 2016/399;

3) «autorità di frontiera»: le guardie di frontiera incaricate, conformemente al diritto nazionale, di procedere alle verifiche di frontiera;

4) «autorità di controllo»: l'autorità di controllo di cui all'articolo 51, paragrafo 1, del regolamento (UE) 2016/679 e l'autorità di controllo di cui all'articolo 41, paragrafo 1, della direttiva (UE) 2016/680;

5) «verifica»: il procedimento di confronto di serie di dati al fine di verificare la validità di una identità dichiarata (verifica «uno a uno»);

6) «identificazione»: il procedimento volto a determinare l'identità di una persona mediante interrogazione di una banca dati confrontando varie serie di dati (verifica «uno a molti»);

7) «dati alfanumerici»: i dati rappresentati da lettere, cifre, caratteri speciali, spazi e segni di punteggiatura;

8) «dati di identità»: i dati di cui all'articolo 27, paragrafo 3, lettere da a) a e);

9) «dati relativi alle impronte digitali»: le immagini delle impronte digitali e le immagini delle impronte digitali latenti che, per il loro carattere di unicità e i punti caratteristici che contengono, permettono confronti precisi e irrefutabili sull'identità di una persona;

10) «immagine del volto», le immagini digitalizzate del volto di una persona;

11) «dati biometrici»: i dati relativi alle impronte digitali o alle immagini del volto o di entrambe;

12) «template biometrico»: la rappresentazione matematica ottenuta estraendo elementi dai dati biometrici, limitatamente alle caratteristiche necessarie per effettuare identificazioni e verifiche;

13) «documento di viaggio»: il passaporto o altro documento equivalente che autorizza il titolare ad attraversare le frontiere esterne e sul quale può essere apposto un visto;

14) «dati del documento di viaggio»: tipo, numero e paese di rilascio del documento di viaggio, data di scadenza della validità del documento di viaggio e codice a tre lettere del paese di rilascio del documento di viaggio;

15) «sistemi di informazione dell'UE»: l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS e l'ECRIS-TCN;

16) «dati Europol»: i dati personali trattati da Europol per le finalità di cui all'articolo 18, paragrafo 2, lettere a), b) e c), del regolamento (UE) 2016/794;

17) «banche dati Interpol»: la banca dati Interpol sui documenti di viaggio rubati o smarriti (banca dati SLTD) e la banca dati Interpol sui documenti di viaggio associati a segnalazioni (banca dati TDAWN);

18) «corrispondenza»: la coincidenza risultante da un confronto automatizzato tra dati personali registrati o in fase di registrazione in un sistema di informazione o in una banca dati;

19) «autorità di polizia»: l'autorità competente quale definita all'articolo 3, punto 7), della direttiva (UE) 2016/680;

20) «autorità designate»: le autorità designate dagli Stati membri, quali definite all'articolo 3, paragrafo 1, punto 26), del regolamento (UE) 2017/2226, all'articolo 2, paragrafo 1, lettera e), della decisione 2008/633/GAI e all'articolo 3, paragrafo 1, punto 21), del regolamento (UE) 2018/1240;

21) «reato di terrorismo», il reato che, ai sensi del diritto nazionale, corrisponde o è equivalente a uno dei reati di cui alla direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio ([35]);

22) «reato grave»: il reato che corrisponde o è equivalente a uno dei reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio ([36]), se è punibile conformemente al diritto nazionale con una pena detentiva o una misura di sicurezza privativa della libertà personale per un periodo massimo di almeno tre anni;

23) «Sistema di ingressi/uscite» o «EES»: il sistema di ingressi/uscite istituito dal regolamento (UE) 2017/2226;

24) «Sistema di informazione visti» o «VIS»: il sistema di informazione visti istituito dal regolamento (CE) n. 767/2008;

25) «Sistema europeo di informazione e autorizzazione ai viaggi» o «ETIAS»: il sistema europeo di informazione e autorizzazione ai viaggi istituito dal regolamento (UE) 2018/1240;

26) «Eurodac»: l'Eurodac istituito dal regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio ([37]);

27) «Sistema di informazione Schengen» o «SIS»: il sistema d'informazione Schengen istituito dai regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862;

28) «ECRIS-TCN»: il sistema centralizzato per l'identificazione degli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi istituito dal regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio ([38]).

Articolo 5

Non discriminazione e diritti fondamentali

Il trattamento di dati personali ai fini del presente regolamento non dà luogo a discriminazioni nei confronti delle persone fondate sul genere, sulla razza, sul colore della pelle o sull'origine etnica o sociale, sulle caratteristiche genetiche, sulla lingua, sulla religione o sulle convinzioni personali, sulle opinioni politiche o di qualsiasi altra natura, sull'appartenenza a una minoranza nazionale, sul patrimonio, sulla nascita, sulla disabilità, sull'età o sull'orientamento sessuale. Esso rispetta pienamente la dignità e l'integrità umana nonché i diritti fondamentali, compreso il diritto al rispetto della vita privata e alla protezione dei dati personali. È prestata particolare attenzione ai minori, alle persone anziane, alle persone con disabilità e alle persone bisognose di protezione internazionale. L'interesse superiore del minore è considerato preminente.

CAPO II

Portale di ricerca europeo

Articolo 6

Portale di ricerca europeo

1. È istituito un portale di ricerca europeo (ESP) al fine di agevolare l'accesso rapido, continuato, efficace, sistematico e controllato delle autorità degli Stati membri e delle agenzie dell'Unione ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol per lo svolgimento dei loro compiti e conformemente ai rispettivi diritti di accesso e agli obiettivi e scopi dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e dell'ECRIS-TCN.

([35]) 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).

([36]) Decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU L 190 del 18.7.2002, pag. 1).

([37]) Regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (GU L 180 del 29.6.2013, pag. 1).

([38]) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (Cfr. pag. 1 della presente Gazzetta ufficiale).

2. L'ESP è composto di:

a) un'infrastruttura centrale, che comprende un portale di ricerca per l'interrogazione simultanea dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS, del sistema ECRIS-TCN, dei dati Europol e delle banche dati Interpol;

b) un canale di comunicazione sicuro tra l'ESP, gli Stati membri e le agenzie dell'Unione autorizzati a usare l'ESP;

c) un'infrastruttura di comunicazione sicura tra l'ESP e l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS centrale, l'ECRIS-TCN, i dati Europol e le banche dati Interpol nonché tra l'ESP e le infrastrutture centrali del CIR e del MID.

3. eu-LISA provvede allo sviluppo dell'ESP e ne assicura la gestione tecnica.

Articolo 7

Uso del portale di ricerca europeo

1. L'uso dell'ESP è riservato alle autorità degli Stati membri e alle agenzie dell'Unione che hanno accesso ad almeno uno dei sistemi di informazione dell'UE conformemente agli strumenti giuridici che disciplinano tali sistemi di informazione dell'UE, al CIR e al MID conformemente al presente regolamento, ai dati Europol conformemente al regolamento (UE) 2016/794 o alle banche dati Interpol conformemente al diritto dell'Unione o nazionale che regola tale accesso.

Dette autorità degli Stati membri e agenzie dell'Unione possono ricorrere all'ESP e ai dati che esso fornisce solo per gli obiettivi e le finalità stabiliti dagli strumenti giuridici che disciplinano tali sistemi di informazione dell'UE, nel regolamento (UE) 2016/794 e nel presente regolamento.

2. Le autorità degli Stati membri e le agenzie dell'Unione di cui al paragrafo 1 usano l'ESP per cercare dati relativi a persone o documenti di viaggio nei sistemi centrali dell'EES, del VIS e dell'ETIAS, conformemente ai rispettivi diritti di accesso conformemente agli strumenti giuridici che disciplinano tali sistemi di informazione dell'UE e al diritto nazionale. Si avvalgono dell'ESP anche per interrogare il CIR, conformemente ai rispettivi diritti di accesso a norma del presente regolamento, ai fini degli articoli 20, 21 e 22.

3. Le autorità degli Stati membri di cui al paragrafo 1 possono usare l'ESP per cercare dati relativi a persone o documenti di viaggio nel SIS centrale di cui ai regolamenti (UE) 2018/1860 e (UE) 2018/1861.

4. Quando previsto a norma del diritto dell'Unione, le agenzie dell'Unione di cui al paragrafo 1 usano l'ESP per cercare nel SIS centrale dati relativi a persone o documenti di viaggio.

5. Le autorità degli Stati membri e le agenzie dell'Unione di cui al paragrafo 1 possono usare l'ESP per cercare dati relativi a documenti di viaggio nelle banche dati Interpol, laddove previsto e conformemente ai rispettivi diritti di accesso a norma del diritto dell'Unione e nazionale.

Articolo 8

Profili per gli utenti del portale di ricerca europeo

1. Al fine di consentire l'uso dell'ESP, eu-LISA crea, in cooperazione con gli Stati membri, un profilo basato su ciascuna categoria di utenti dell'ESP e sulle finalità delle loro interrogazioni, secondo le modalità tecniche e i diritti di accesso di cui al paragrafo 2. Ogni profilo comprende, conformemente al diritto dell'Unione e nazionale, le seguenti informazioni:

a) i campi di dati da usare per l'interrogazione;

b) i sistemi di informazione dell'UE, i dati Europol e le banche dati Interpol che sono o possono essere interrogati e che forniscono una risposta all'utente;

c) i dati specifici contenuti nei sistemi di informazione dell'UE, i dati Europol e le banche dati Interpol che possono essere interrogati;

d) le categorie di dati che possono essere forniti in ciascuna risposta.

2. La Commissione adotta atti di esecuzione per specificare le modalità tecniche dei profili di cui al paragrafo 1, nel rispetto dei diritti di accesso degli utenti dell'ESP conformemente agli strumenti giuridici che disciplinano i sistemi di informazione dell'UE e al diritto nazionale. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

3. I profili di cui al paragrafo 1 sono riesaminati periodicamente da eu-LISA in cooperazione con gli Stati membri, almeno una volta all'anno, e aggiornati se necessario.

Articolo 9

Interrogazioni

1. Gli utenti dell'ESP avviano un'interrogazione presentando dati alfanumerici o biometrici all'ESP. Ove un'interrogazione sia stata lanciata, l'ESP interroga simultaneamente l'EES, l'ETIAS, il VIS, il SIS, l'Eurodac, l'ECRIS-TCN, il CIR, i dati Europol e le banche dati Interpol, usando i dati presentati dall'utente e in funzione del profilo dell'utente.

2. Le categorie di dati usati per avviare l'interrogazione tramite l'ESP corrispondono alle categorie di dati relativi a persone o documenti di viaggio che possono essere usati per interrogare i vari sistemi di informazione dell'UE, i dati Europol e le banche dati Interpol conformemente agli strumenti giuridici che li disciplinano.

3. eu-LISA, in cooperazione con gli Stati membri, implementa un documento di controllo dell'interfaccia per l'ESP basato sul formato universale dei messaggi di cui all'articolo 38.

4. Ove un'interrogazione sia stata lanciata da un utente dell'ESP, l'EES, l'ETIAS, il VIS, il SIS, l'Eurodac, il ECRIS-TCN, il CIR, il MID, i dati Europol e le banche dati Interpol risponde all'interrogazione fornendo i dati in essi contenuti.

Fatto salvo l'articolo 20, la risposta fornita dall'ESP indica il sistema di informazione dell'UE o la banca dati cui appartengono i dati.

L'ESP non fornisce alcuna informazione in merito ai dati contenuti nei sistemi di informazione dell'UE, ai dati Europol e alla banca dati Interpol a cui l'utente non ha accesso a norma del diritto dell'Unione e nazionale applicabile.

5. L'ESP è progettato in modo da garantire che le interrogazioni delle banche dati Interpol lanciate attraverso l'ESP siano effettuate in modo tale che nessuna informazione sia rivelata al titolare della segnalazione Interpol.

6. L'ESP fornisce risposte all'utente non appena i dati sono disponibili in uno dei sistemi di informazione dell'UE, nei dati Europol o nelle banche dati Interpol. Tali risposte contengono unicamente i dati a cui l'utente ha accesso a norma del diritto dell'Unione e nazionale.

7. La Commissione adotta un atto di esecuzione per specificare la procedura tecnica di interrogazione da parte dell'ESP dei sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol e il formato delle risposte dell'ESP. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 10

Registrazioni

1. Fatti salvi l'articolo 46 del regolamento (UE) 2017/2226, l'articolo 34 del regolamento (CE) n. 767/2008, l'articolo 69 del regolamento (UE) 2018/1240 e gli articoli 12 e 18 del regolamento (UE) 2018/1861, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nell'ESP. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che effettua l'interrogazione e il profilo ESP usato;

b) la data e l'ora dell'interrogazione;

c) i sistemi di informazione dell'UE e le banche dati Interpol interrogati.

2. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tali autorità debitamente autorizzato a usare l'ESP. Ciascuna agenzia dell'Unione conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato.

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi. Dette registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Ove, tuttavia, esse siano necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando non sono più necessarie per le procedure di monitoraggio.

Articolo 11

Procedure sostitutive in caso di impossibilità tecnica dell'uso del portale di ricerca europeo

1. Qualora sia tecnicamente impossibile usare l'ESP per interrogare uno o più sistemi di informazione dell'UE o il CIR a causa di un guasto dell'ESP, eu-LISA informa gli utenti del portale in modo automatizzato.

2. Qualora sia tecnicamente impossibile usare l'ESP per interrogare uno o più sistemi di informazione dell'UE o il CIR a causa di un guasto dell'infrastruttura nazionale di uno Stato membro, tale Stato membro ne informa eu-LISA e la Commissione in modo automatizzato.

3. Nei casi di cui ai paragrafi 1 o 2 del presente articolo, fintantoché il guasto tecnico non è riparato, l'obbligo di cui all'articolo 7, paragrafi 2 e 4, non si applica e gli Stati membri accedono direttamente ai sistemi di informazione dell'UE o al CIR quando sono tenuti a farlo a norma del diritto nazionale o dell'Unione.

4. Qualora sia tecnicamente impossibile usare l'ESP per interrogare uno o più sistemi di informazione dell'UE o il CIR a causa di un guasto dell'infrastruttura di un'agenzia dell'Unione, l'agenzia in questione ne informa eu-LISA e la Commissione in modo automatizzato.

CAPO III

Servizio comune di confronto biometrico

Articolo 12

Servizio comune di confronto biometrico

1. Al fine di sostenere il CIR e il MID nonché gli obiettivi dell'EES, del VIS, dell'Eurodac, del SIS e dell'ECRIS-TCN è istituito un servizio comune di confronto biometrico (BMS comune) che conserva i template biometrici ottenuti dai dati biometrici di cui all'articolo 13 registrati nel CIR e nel SIS e consente di effettuare interrogazioni con dati biometrici trasversalmente in più sistemi di informazione dell'UE.

2. Il BMS comune è composto di:

a) un'infrastruttura centrale, che sostituisce i sistemi centrali rispettivamente dell'EES, del VIS, del SIS, dell'Eurodac e dell'ECRIS-TCN nella misura in cui registri template biometrici e consenta di effettuare interrogazioni con dati biometrici;

b) un'infrastruttura di comunicazione sicura tra il BMS comune, il SIS centrale e il CIR.

3. eu-LISA provvede allo sviluppo del BMS comune e ne assicura la gestione tecnica.

Articolo 13

Conservazione di template biometrici nel servizio comune di confronto biometrico

1. Il BMS comune conserva i template biometrici, che ottiene dai seguenti dati biometrici:

a) i dati di cui all'articolo 16, paragrafo 1, lettera d), all'articolo 17, paragrafo 1, lettere b) e c), e all'articolo 18, paragrafo 2, lettere a), b) e c), del regolamento (UE) 2017/2226;

b) i dati di cui all'articolo 9, punto 6), del regolamento (CE) n. 767/2008;

c) i dati di cui all'articolo 20, paragrafo 2, lettere w) e x), esclusi i dati relativi alle impronte palmari, del regolamento (UE) 2018/1861;

d) la raccolta di dati di cui all'articolo 4, paragrafo 1, lettere u) e v), esclusi i dati relativi alle impronte palmari, del regolamento (UE) 2018/1860.

I template biometrici sono conservati nel BMS comune separati per logica in base al sistema di informazione dell'UE da cui provengono i dati.

2. Per ciascuna serie di dati di cui al paragrafo 1, il BMS comune inserisce in ogni template biometrico un riferimento ai sistemi di informazione dell'UE in cui sono conservati i corrispondenti dati biometrici e un riferimento alle effettive registrazioni in tali sistemi di informazione dell'UE.

3. I template biometrici sono inseriti nel servizio BMS comune solo dopo che questo ha effettuato un controllo automatizzato della qualità dei dati biometrici aggiunti in uno dei sistemi di informazione dell'UE al fine di accertare il rispetto di norme minime di qualità dei dati.

4. La conservazione dei dati di cui al paragrafo 1 rispetta le norme di qualità di cui all'articolo 37, paragrafo 2.

5. La Commissione stabilisce, mediante un atto di esecuzione, i requisiti di prestazione e le modalità pratiche per il monitoraggio delle prestazioni del BMS comune, al fine di garantire che l'efficacia delle ricerche biometriche rispetti procedure critiche in termini di tempo quali i controlli di frontiera e le identificazioni. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 14

Ricerca di dati biometrici tramite il servizio comune di confronto biometrico

Per la ricerca dei dati biometrici conservati al loro interno, il CIR e il SIS usano i template biometrici conservati nel BMS comune. Le interrogazioni con dati biometrici sono effettuate per le finalità del presente regolamento e dei regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 e (UE) 2019/816.

Articolo 15

Periodo di conservazione dei dati nel servizio comune di confronto biometrico

I dati di cui all'articolo 13, paragrafi 1 e 2, sono conservati nel BMS comune soltanto per il tempo in cui i corrispondenti dati biometrici sono conservati nel CIR o nel SIS. Tali dati sono cancellati dal BMS comune in modo automatizzato.

Articolo 16

Registrazioni

1. Fatti salvi l'articolo 46 del regolamento (UE) 2017/2226, l'articolo 34 del regolamento (CE) n. 767/2008 e gli articoli 12 e 18 del regolamento (UE) 2018/1861, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nel BMS comune. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che ha effettuato l'interrogazione;

b) lo storico della creazione e della conservazione dei template biometrici;

c) i sistemi di informazione dell'UE interrogati con i template biometrici conservati nel BMS comune;

d) la data e l'ora dell'interrogazione;

e) il tipo di dati biometrici usati per avviare l'interrogazione;

f) i risultati dell'interrogazione e la data e l'ora del risultato;

2. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tale autorità debitamente autorizzato a usare il BMS comune. Ciascuna agenzia dell'Unione conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato.

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi ai sensi dell'articolo 42. Dette registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Qualora, tuttavia, siano necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando non sono più necessarie per le procedure di monitoraggio.

CAPO IV

Archivio comune di dati di identità

Articolo 17

Archivio comune di dati di identità

1. Al fine di agevolare e contribuire alla corretta identificazione delle persone registrate nell'EES, nel VIS, nell'ETIAS, nell'Eurodac e nell'ECRIS-TCN conformemente all'articolo 20, di sostenere il funzionamento del MID conformemente all'articolo 21 e di agevolare e semplificare alle autorità designate e a Europol l'accesso all'EES, al VIS, all'ETIAS, e Eurodac quando necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi conformemente all'articolo 22, è istituito un archivio comune di dati di identità (CIR) che, per ciascuna persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nell'ECRIS-TCN, crea un fascicolo individuale contenente i dati di cui all'articolo 18.

2. Il CIR è composto di:

a) un'infrastruttura centrale che sostituisce i sistemi centrali dell'EES, del VIS, dell'ETIAS, dell'Eurodac e dell'ECRIS-TCN, rispettivamente, nella misura in cui conserva i dati di cui all'articolo 18;

b) un canale di comunicazione sicuro tra il CIR, gli Stati membri e le agenzie dell'Unione autorizzate a usare il CIR conformemente al diritto dell'Unione e nazionale;

c) un'infrastruttura di comunicazione sicura tra il CIR e l'EES, il VIS, l'ETIAS, l'Eurodac e l'ECRIS-TCN, nonché le infrastrutture centrali dell'ESP, del BMS comune e del MID.

3. eu-LISA provvede allo sviluppo del CIR e ne assicura la gestione tecnica.

4. Qualora, a causa di un guasto del CIR, sia tecnicamente impossibile interrogare tale archivio ai fini dell'identificazione di una persona conformemente all'articolo 20, a fini di individuazione di identità multiple a norma dell'articolo 21 o a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi a norma dell'articolo 22, eu-LISA ne informa gli utenti del CIR in modo automatizzato.

5. eu-LISA, in cooperazione con gli Stati membri, implementa un documento di controllo dell'interfaccia per il CIR basato sul formato universale dei messaggi di cui all'articolo 38.

Articolo 18

Dati dell'archivio comune di dati di identità

1. Il CIR conserva i seguenti dati, separati per logica in base al sistema di informazione di provenienza dei dati:

a) i dati di cui all'articolo 16, paragrafo 1, lettere da a) a d), all'articolo 17, paragrafo 1, lettere a), b) e c), e all'articolo 18, paragrafi 1 e 2, del regolamento (UE) 2017/2226;

b) i dati di cui all'articolo 9, punti 4, lettere da a) a c), 5 e 6, del regolamento (CE) n. 767/2008;

c) i dati di cui all'articolo 17, punto 2), lettere da a) a e), del regolamento (UE) 2018/1240.

2. Per ciascuna serie di dati di cui al paragrafo 1 il CIR inserisce un riferimento ai sistemi di informazione dell'UE cui appartengono i dati.

3. Le autorità che hanno accesso al CIR effettuano tale accesso conformemente ai rispettivi diritti di accesso a norma degli strumenti giuridici che disciplinano i sistemi di informazione dell'UE e a norma del diritto nazionale e conformemente ai rispettivi diritti di accesso a norma del presente regolamento, ai fini di cui agli articoli 20, 21 e 22.

4. Per ciascuna serie di dati di cui al paragrafo 1 il CIR inserisce un riferimento all'effettiva registrazione nei sistemi di informazione dell'UE cui appartengono i dati.

5. La conservazione dei dati di cui al paragrafo 1 rispetta le norme di qualità di cui all'articolo 37, paragrafo 2.

Articolo 19

Aggiunta, modifica e cancellazione di dati nell'archivio comune di dati di identità

1. Qualora nell'EES, nel VIS e nell'ETIAS siano aggiunti, modificati o cancellati dati, sono aggiunti, modificati o cancellati di conseguenza, in modo automatizzato, i dati di cui all'articolo 18 conservati nel fascicolo individuale del CIR.

2. Qualora sia creato un collegamento bianco o rosso nel MID, conformemente all'articolo 32 o all'articolo 33, tra i dati di due o più sistemi di informazione dell'UE che compongono il CIR, quest'ultimo non crea un nuovo fascicolo individuale, bensì aggiunge i nuovi dati al fascicolo individuale dei dati oggetto del collegamento.

Articolo 20

Accesso all'archivio comune di dati di identità a fini di identificazione

1. Le interrogazioni del CIR sono effettuate da un'autorità di polizia conformemente ai paragrafi 2 e 5 unicamente nei seguenti casi:

a) se l'autorità di polizia non è in grado di identificare una persona in ragione dell'assenza di un documento di viaggio o di un altro documento credibile che ne provi l'identità;

b) se sussistono dubbi quanto ai dati di identità forniti da una persona;

c) se sussistono dubbi quanto all'autenticità del documento di viaggio o di un altro documento credibile fornito da una persona;

d) se sussistono dubbi quanto all'identità del titolare del documento di viaggio o di un altro documento credibile; ovvero

e) se l'interessato non è in grado o rifiuta di cooperare.

Tali interrogazioni non sono autorizzate nel caso di minori di età inferiore a 12 anni, a meno che ciò non sia nell'interesse superiore del minore.

2. Qualora si verifichi una delle circostanze di cui al paragrafo 1, l'autorità di polizia appositamente autorizzata da una misura legislativa nazionale di cui al paragrafo 5 può, unicamente ai fini dell'identificazione di una persona, interrogare il CIR con i dati biometrici dell'interessato acquisiti sul posto durante una verifica d'identità, a condizione che la procedura sia stata avviata in presenza dell'interessato.

3. Se dall'interrogazione risulta che nell'archivio comune sono conservati dati dell'interessato, l'autorità di polizia ha accesso all'archivio comune per consultare i dati di cui all'articolo 18, paragrafo 1.

Se non possono essere usati i dati biometrici dell'interessato o se l'interrogazione con tali dati non dà esito, l'interrogazione è effettuata con i dati di identità dell'interessato combinati con i dati del documento di viaggio oppure con i dati di identità forniti dall'interessato.

4. L'autorità di polizia appositamente autorizzata da una misura legislativa nazionale di cui al paragrafo 6 può, in caso di catastrofe naturale, incidente o attacco terroristico e unicamente ai fini dell'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati, interrogare il CIR con i dati biometrici degli interessati.

5. Gli Stati membri che intendono valersi della possibilità offerta dal paragrafo 2 adottano misure legislative nazionali. Nell'adottare tali misure gli Stati membri tengono conto della necessità di evitare qualsiasi discriminazione nei confronti di cittadini di paesi terzi. Tali misure specificano le finalità esatte dell'identificazione nell'ambito degli obiettivi di cui all'articolo 2, paragrafo 1, lettere b) e c). Designano le autorità di polizia competenti e stabiliscono le procedure, le condizioni e i criteri di tali verifiche.

6. Gli Stati membri che intendono valersi della possibilità offerta dal paragrafo 4 adottano misure legislative nazionali che stabiliscono le procedure, le condizioni e i criteri.

Articolo 21

Accesso all'archivio comune di dati di identità a fini di individuazione di identità multiple

1. Se un'interrogazione del CIR dà luogo a un collegamento giallo conformemente all'articolo 28, paragrafo 4, l'autorità responsabile della verifica manuale delle identità diverse conformemente all'articolo 29 ha accesso, unicamente ai fini della verifica, ai dati di cui all'articolo 18, paragrafi 1 e 2, conservati nel CIR interessati dal collegamento giallo.

2. Se un'interrogazione del CIR dà luogo a un collegamento rosso conformemente all'articolo 32, le autorità di cui all'articolo 26, paragrafo 2, hanno accesso, unicamente al fine di combattere la frode di identità, ai dati di cui all'articolo 18, paragrafi 1 e 2, conservati nel CIR interessati dal collegamento rosso.

Articolo 22

Interrogazione dell'archivio comune di dati di identità a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi

1. Se in un caso specifico vi sono fondati motivi per ritenere che la consultazione dei sistemi di informazione dell'UE contribuisca alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o di altri reati gravi, in particolare laddove sussista il sospetto che i dati dell'autore presunto o effettivo oppure della vittima di un reato di terrorismo o di altri reati gravi siano conservati nell'EES, nel VIS o nell'ETIAS, le autorità designate e Europol possono consultare il CIR per sapere se nell'EES, nel VIS o nell'ETIAS sono presenti dati su una determinata persona.

2. Se nell'EES, nel VIS o nell'ETIAS sono presenti dati sulla persona in questione, il CIR risponde all'interrogazione fornendo alle autorità designate e a Europol un riferimento di cui all'articolo 18, paragrafo 2, al sistema di informazione dell'UE che contiene i corrispondenti dati. Il CIR risponde con modalità che non compromettano la sicurezza dei dati.

La risposta che indica che i dati sulla persona in questione sono presenti in uno dei sistemi di informazione dell'UE di cui al paragrafo 1 è utilizzata solo per presentare una richiesta di accesso integrale soggetta alle condizioni e alle procedure stabilite dai rispettivi strumenti giuridici che disciplinano tale accesso.

In caso di una o più corrispondenze, l'autorità designata o Europol richiede il pieno accesso ad almeno uno dei sistemi di informazione dai quali è emersa una corrispondenza.

Ove, in via eccezionale, tale accesso integrale non sia richiesto, le autorità designate registrano la motivazione per la mancata richiesta nel fascicolo nazionale. Europol registra la motivazione nel pertinente fascicolo.

3. Il pieno accesso ai dati contenuti nell'EES, nel VIS o nell'ETIAS a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi è soggetto alle condizioni e procedure previste nei rispettivi strumenti giuridici che disciplinano tale accesso.

Articolo 23

Periodo di conservazione dei dati nell'archivio comune di dati di identità

1. I dati di cui all'articolo 18, paragrafi 1, 2 e 4, sono cancellati in modo automatizzato dal CIR conformemente alle disposizioni in materia di conservazione dei dati dei regolamenti (UE) 2017/2226, (CE) n. 767/2008 e (UE) 2018/1240 rispettivamente.

2. Il fascicolo individuale è conservato nel CIR soltanto per il tempo in cui i corrispondenti dati sono conservati in almeno uno dei sistemi di informazione dell'UE i cui dati sono contenuti nel CIR. La creazione di un collegamento non incide sul periodo di conservazione di ciascuno dei singoli dati oggetto del collegamento.

Articolo 24

Registrazioni

1. Fatti salvi l'articolo 46 del regolamento (UE) 2017/2226, l'articolo 34 del regolamento (CE) n. 767/02008 e l'articolo 69 del regolamento (UE) 2017/1240, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nel CIR conformemente ai paragrafi 2, 3 e 4 del presente articolo.

2. eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati ai sensi dell'articolo 20 effettuate nel CIR. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che ha avviato l'interrogazione;

b) la finalità dell'accesso dell'utente che effettua l'interrogazione tramite il CIR;

c) la data e l'ora dell'interrogazione;

d) il tipo di dati usati per avviare l'interrogazione;

e) i risultati dell'interrogazione.

3. eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati ai sensi dell'articolo 21 nel CIR. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che ha avviato l'interrogazione;

b) la finalità dell'accesso dell'utente che effettua l'interrogazione tramite il CIR;

c) la data e l'ora dell'interrogazione;

d) ove sia creato un collegamento, i dati usati per avviare l'interrogazione e i risultati dell'interrogazione con indicazione del sistema di informazione dell'UE da cui sono stati ottenuti i dati.

4. eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati ai sensi dell'articolo 22 nel CIR. Tali registrazioni comprendono i seguenti elementi:

a) la data e l'ora dell'interrogazione;

b) i dati usati per avviare l'interrogazione;

c) i risultati dell'interrogazione;

d) lo Stato membro o l'agenzia dell'Unione che ha effettuato l'interrogazione del CIR.

Le autorità di controllo competenti, conformemente all'articolo 41 della direttiva (UE) 2016/680, o il garante europeo della protezione dei dati, conformemente all'articolo 43 del regolamento (UE) 2016/794, verificano periodicamente, a intervalli non superiori a sei mesi, le registrazioni dell'accesso per controllare il rispetto delle procedure e delle condizioni di cui all'articolo 22, paragrafi 1 e 2, del presente regolamento.

5. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tali autorità debitamente autorizzato a usare il CIR ai sensi degli articoli 20, 21 e 22. Ciascuna agenzia dell'Unione conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato ai sensi degli articoli 21 e 22.

Inoltre, per qualsiasi accesso al CIR ai sensi dell'articolo 22, ciascuno Stato membro conserva le seguenti registrazioni:

a) il riferimento del fascicolo nazionale;

b) la finalità dell'accesso;

c) conformemente alle disposizioni nazionali, l'identità utente esclusiva del funzionario che ha effettuato l'interrogazione e del funzionario che ha ordinato l'interrogazione.

6. Conformemente al regolamento (UE) 2016/794, per qualsiasi accesso al CIR ai sensi dell'articolo 22 del presente regolamento, Europol conserva le registrazioni dell'identità utente esclusiva del funzionario che ha effettuato l'interrogazione e del funzionario che ha ordinato l'interrogazione.

7. Le registrazioni di cui ai paragrafi da 2 a 6 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi. Tali registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Qualora, tuttavia, siano necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando le procedure di monitoraggio non necessitano più di tali registrazioni.

8. eu-LISA conserva le registrazioni relative allo storico dei dati conservati nei fascicoli individuali. eu-LISA cancella tali registrazioni, in modo automatizzato, non appena sono cancellati i dati.

CAPO V

Rilevatore di identità multiple

Articolo 25

Rilevatore di identità multiple

1. Al fine di sostenere il funzionamento del CIR e gli obiettivi dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e dell'ECRIS-TCN è istituito un rilevatore di identità multiple (MID) che crea e conserva un fascicolo di conferma dell'identità, di cui all'articolo 34, contenente collegamenti tra i dati dei sistemi di informazione dell'UE inclusi nel CIR e i dati del SIS e che, di conseguenza, rileva le identità multiple, al duplice scopo di agevolare le verifiche di identità e contrastare la frode di identità.

2. Il MID è composto di:

a) un'infrastruttura centrale che conserva i collegamenti e i riferimenti ai sistemi di informazione dell'UE;

b) un'infrastruttura di comunicazione sicura che collega il MID al SIS e alle infrastrutture centrali dell'ESP e del CIR.

3. eu-LISA provvede allo sviluppo del MID e ne assicura la gestione tecnica.

Articolo 26

Accesso al rilevatore di identità multiple

1. Ai fini della verifica manuale delle identità diverse di cui all'articolo 29, l'accesso ai dati di cui all'articolo 34 conservati nel MID è concesso:

a) alle autorità competenti designate a norma dell'articolo 9, paragrafo 2, del regolamento (UE) 2017/2226 quando creano o aggiornano un fascicolo individuale nell'EES conformemente all'articolo 14 di tale regolamento;

b) alle autorità competenti per i visti di cui all'articolo 6, paragrafo 1, del regolamento (CE) n. 767/2008 quando creano o aggiornano un fascicolo relativo alla domanda nel VIS conformemente a tale regolamento;

c) all'unità centrale ETIAS e alle unità nazionali ETIAS quando effettuano il trattamento di cui agli articoli 22 e 26 del regolamento (UE) 2018/1240;

d) all'ufficio SIRENE degli Stati membri che creano o aggiornano una segnalazione SIS conformemente ai regolamenti (UE) 2018/1860 e (UE) 2018/1861.

2. Le autorità degli Stati membri e le agenzie dell'Unione che hanno accesso ad almeno uno dei sistemi di informazione dell'UE inclusi nel CIR o al SIS hanno accesso ai dati di cui all'articolo 34, lettere a) e b), riguardanti i collegamenti rossi di cui all'articolo 32.

3. Le autorità degli Stati membri e le agenzie dell'Unione hanno accesso ai collegamenti bianchi di cui all'articolo 33 se hanno accesso ai due sistemi di informazione dell'UE che contengono dati tra i quali è stato creato il collegamento bianco.

4. Le autorità degli Stati membri e le agenzie dell'Unione hanno accesso ai collegamenti verdi di cui all'articolo 31 se hanno accesso ai due sistemi di informazione dell'UE che contengono dati tra i quali è stato creato il collegamento verde e se dall'interrogazione di tali sistemi di informazione è emersa una corrispondenza tra le due serie di dati oggetto del collegamento.

Articolo 27

Rilevazione di identità multiple

1. È avviata una procedura di rilevazione di identità multiple nel CIR e nel SIS quando:

a) è creato o aggiornato un fascicolo individuale nell'EES conformemente all'articolo 14 del regolamento (UE) 2017/2226;

b) è creato o aggiornato un fascicolo relativo alla domanda nel VIS conformemente al regolamento (CE) n. 767/2008;

c) è creato o aggiornato un fascicolo di domanda nell'ETIAS conformemente all'articolo 19 del regolamento (UE) 2018/1240;

d) è creata o aggiornata una segnalazione su una persona nel SIS conformemente all'articolo 3 del regolamento (UE) 2018/1860 e al capo V del regolamento (UE) 2018/1861.

2. Se tra i dati di un sistema di informazione dell'UE di cui al paragrafo 1 figurano dati biometrici, il CIR e il SIS centrale effettuano la procedura di rilevazione delle identità multiple tramite il BMS comune. Il BMS comune raffronta i template biometrici ricavati dai nuovi dati biometrici con i template biometrici già presenti al suo interno e verifica se nel CIR o nel SIS centrale sono già conservati dati della stessa persona.

3. Oltre alla procedura di cui al paragrafo 2, il CIR e il SIS centrale effettuano la ricerca nei dati conservati, rispettivamente, nel SIS centrale e nel CIR mediante l'ESP usando i seguenti dati:

a) cognome; nome o nomi; data di nascita; cittadinanza o cittadinanze; e sesso, conformemente all'articolo 16, paragrafo 1, lettera a), all'articolo 17, paragrafo 1, e all'articolo 18, paragrafo 1, del regolamento (UE) 2017/2226;

b) cognome; nome o nomi; data di nascita; sesso; luogo e paese di nascita; e cittadinanze, conformemente all'articolo 9, punto 4), lettere a) e a a *bis*), del regolamento (CE) n. 767/2008;

c) cognome; nome o nomi; cognome alla nascita; «alias»; data di nascita, luogo di nascita, sesso e attuale cittadinanza, conformemente all'articolo 17, paragrafo 2, del regolamento (UE) 2018/1240;

d) cognomi; nomi; nomi e cognomi alla nascita, eventuali nomi e cognomi precedenti e «alias»; luogo di nascita, data di nascita, genere e ogni cittadinanza posseduta, conformemente all'articolo 20, paragrafo 2, del regolamento (UE) 2018/1861;

e) cognomi, nomi, nomi e cognomi alla nascita, eventuali nomi e cognomi precedenti e «alias»; luogo di nascita, data di nascita, genere e ogni posseduta, conformemente all'articolo 4 del regolamento (UE) 2018/1860.

4. Oltre alla procedura di cui ai paragrafi 2 e 3, il CIR e il SIS centrale effettuano la ricerca nei dati conservati, rispettivamente, nel CIR e nel SIS centrale mediante l'ESP usando i dati del documento di viaggio.

5. La procedura di rilevazione di identità multiple è avviata unicamente per confrontare i dati disponibili in un sistema di informazione dell'UE con i dati disponibili negli altri sistemi di informazione dell'UE.

Articolo 28

Esito della procedura di rilevazione di identità multiple

1. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, non risulti alcuna corrispondenza, le procedure di cui all'articolo 27, paragrafo 1, proseguono conformemente agli strumenti giuridici che le disciplinano.

2. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, risultino una o più corrispondenze, il CIR e, se del caso, il SIS creano un collegamento tra i dati usati per avviare l'interrogazione e i dati per i quali è emersa la corrispondenza.

Qualora risultino più corrispondenze è creato un collegamento tra tutti i dati per i quali è emersa una corrispondenza. Se i dati sono già oggetto di un collegamento, questo è esteso ai dati usati per avviare l'interrogazione.

3. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, risultino una o più corrispondenze e i dati di identità dei fascicoli oggetto del collegamento siano identici o simili, è creato un collegamento bianco conformemente all'articolo 33.

4. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, risultino una o più corrispondenze e i dati di identità dei fascicoli oggetto del collegamento non possano essere considerati simili, è creato un collegamento giallo conformemente all'articolo 30 e si applica la procedura di cui all'articolo 29.

5. La Commissione adotta atti delegati conformemente all'articolo 73 per stabilire le procedure per determinare i casi in cui è possibile considerare che i dati di identità sono identici o simili.

6. I collegamenti sono conservati nel fascicolo di conferma dell'identità di cui all'articolo 34.

7. La Commissione, in collaborazione con eu-LISA, stabilisce con atti di esecuzione le norme tecniche per creare i collegamenti tra i dati di diversi sistemi di informazione dell'UE. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 29

Verifica manuale delle identità diverse e autorità responsabili

1. Fatto salvo il paragrafo 2, l'autorità responsabile della verifica manuale delle identità diverse è:

a) l'autorità competente designata a norma dell'articolo 9, paragrafo 2, del regolamento (UE) 2017/2226, per le corrispondenze emerse durante la creazione o l'aggiornamento di un fascicolo individuale nell'EES conformemente a tale regolamento;

b) le autorità competenti per i visti di cui all'articolo 6, paragrafo 1, del regolamento (CE) n. 767/2008, per le corrispondenze emerse durante la creazione o l'aggiornamento di un fascicolo relativo alla domanda nel VIS conformemente a tale regolamento;

c) l'unità centrale ETIAS e le unità nazionali ETIAS, per le corrispondenze emerse durante la creazione o l'aggiornamento di un fascicolo di domanda conformemente al regolamento (UE) 2018/1240;

d) l'ufficio SIRENE degli Stati membri, per le corrispondenze emerse durante la creazione o l'aggiornamento di una segnalazione SIS conformemente ai regolamenti (UE) 2018/1860 e (UE) 2018/1861.

Il MID indica l'autorità responsabile della verifica manuale delle identità diverse nel fascicolo di conferma dell'identità.

2. L'autorità responsabile della verifica manuale delle identità diverse nel fascicolo di conferma dell'identità è l'ufficio SIRENE dello Stato membro che ha creato la segnalazione qualora sia creato un collegamento ai dati contenuti in una segnalazione:

a) di persone ricercate per l'arresto a fini di consegna o di estradizione di cui all'articolo 26 del regolamento (UE) 2018/1862;

b) di persone scomparse o vulnerabili di cui all'articolo 32 del regolamento (UE) 2018/1862;

c) di persone ricercate per presenziare a un procedimento giudiziario di cui all'articolo 34 del regolamento (UE) 2018/1862;

d) di persone ai fini di controlli discreti, controlli di indagine o controlli specifici di cui all'articolo 36 del regolamento (UE) 2018/1862.

3. Fatto salvo il paragrafo 4 del presente articolo, l'autorità responsabile della verifica manuale delle identità diverse ha accesso ai dati oggetto del collegamento contenuti nel pertinente fascicolo di conferma dell'identità e ai dati di identità oggetto del collegamento nel CIR e, se del caso, nel SIS. Essa esamina senza indugio le identità diverse. Una volta completata tale valutazione, l'autorità responsabile aggiorna il collegamento conformemente agli articoli 31, 32 e 33 e lo aggiunge senza indugio al fascicolo di conferma dell'identità.

4. Se l'autorità responsabile della verifica manuale delle identità diverse nel fascicolo di conferma dell'identità è l'autorità competente designata a norma dell'articolo 9, paragrafo 2, del regolamento (UE) 2017/2226, che crea o aggiorna un fascicolo individuale nell'EES conformemente all'articolo 14 di tale regolamento, e qualora sia creato un collegamento giallo, tale autorità effettua ulteriori verifiche. Unicamente per tale scopo, detta autorità ha accesso ai corrispondenti dati di identità contenuti nel pertinente fascicolo di conferma dell'identità. Essa esamina le identità diverse, aggiorna il collegamento conformemente agli articoli 31, 32 e 33 del presente regolamento e lo aggiunge senza indugio al fascicolo di conferma dell'identità.

Tale verifica manuale delle identità diverse è avviata in presenza dell'interessato, al quale è offerta la possibilità di spiegare le circostanze all'autorità responsabile, che tiene conto di tali spiegazioni.

Nel caso in cui la verifica manuale delle identità diverse sia svolta alla frontiera, essa avviene, ove possibile, entro 12 ore dalla creazione di un collegamento giallo a norma dell'articolo 28, paragrafo 4.

5. Qualora sia creato più di un collegamento, l'autorità responsabile della verifica manuale delle identità diverse esamina ogni collegamento separatamente.

6. Se i dati per i quali risulta una corrispondenza sono stati già oggetto di un collegamento, l'autorità responsabile della verifica manuale delle identità diverse valuta la creazione di nuovi collegamenti tenendo conto dei collegamenti esistenti.

Articolo 30

Collegamento giallo

1. Qualora non sia stata svolta alcuna verifica manuale delle identità diverse, un collegamento tra dati di due o più sistemi di informazione dell'UE è classificato giallo nei seguenti casi:

a) il collegamento evidenzia gli stessi dati biometrici ma ha dati di identità simili o differenti;

b) il collegamento evidenzia dati di identità differenti ma condivide gli stessi dati del documento di viaggio e almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici della persona in questione;

c) il collegamento evidenzia gli stessi dati di identità ma ha dati biometrici differenti;

d) il collegamento ha dati di identità simili o differenti, evidenzia gli stessi dati del documento di viaggio, ma ha dati biometrici differenti.

2. Quando un collegamento è classificato giallo conformemente al paragrafo 1 si applica la procedura di cui all'articolo 29.

Articolo 31

Collegamento verde

1. Il collegamento tra dati di due o più sistemi di informazione dell'UE è classificato verde quando:

a) evidenzia dati biometrici differenti ma gli stessi dati di identità e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse;

b) evidenzia dati biometrici differenti, dati di identità simili o differenti, lo stesso documento di viaggio e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse;

c) evidenzia dati di identità differenti ma lo stesso documento di viaggio, almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici sulla persona in questione e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse.

2. Quando è interrogato il CIR o il SIS e sussiste un collegamento verde tra i dati in due o più sistemi di informazione dell'UE, il MID indica che i dati di identità oggetto del collegamento non si riferiscono alla stessa persona.

3. Se l'autorità di uno Stato membro dispone di prove indicanti che un collegamento verde sia stato incorrettamente registrato nel MID, non è aggiornato o che i dati sono stati trattati nel MID o nei sistemi di informazione dell'UE in violazione del presente regolamento, essa controlla i dati pertinenti conservati nel CIR e nel SIS e, se necessario, rettifica o cancella senza indugio il collegamento dal MID. L'autorità dello Stato membro informa senza indugio lo Stato membro responsabile della verifica manuale delle identità diverse.

Articolo 32

Collegamento rosso

1. Il collegamento tra dati di due o più sistemi di informazione dell'UE è classificato rosso nei seguenti casi:

a) il collegamento evidenzia gli stessi dati biometrici ma dati di identità simili o differenti e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono alla stessa persona in maniera ingiustificata;

b) il collegamento evidenzia dati di identità identici, simili o differenti e lo stesso documento di viaggio ma dati biometrici differenti e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse e che almeno una delle due persone usa in maniera ingiustificata lo stesso documento di viaggio;

c) il collegamento evidenzia gli stessi dati di identità ma dati biometrici differenti e i dati relativi al documento di viaggio sono differenti o assenti, e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse che usano le identità in questione in maniera ingiustificata;

d) il collegamento evidenzia gli stessi dati di identità e lo stesso documento di viaggio, almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici sulla persona in questione e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono alla stessa persona in maniera ingiustificata.

2. Quando è interrogato il CIR o il SIS e sussiste un collegamento rosso tra i dati di due o più sistemi di informazione dell'UE, il MID indica i dati di cui all'articolo 34. Al collegamento rosso è dato seguito conformemente al diritto dell'Unione e nazionale, basando ogni conseguenza giuridica per la persona in questione solamente sui dati pertinenti relativi a tale persona. Dalla mera esistenza di un collegamento rosso non deriva alcuna conseguenza giuridica per la persona in questione.

3. Qualora sia creato un collegamento rosso tra dati dell'EES, del VIS, dell'ETIAS, dell'Eurodac o dell'ECRIS-TCN, il fascicolo individuale conservato nel CIR è aggiornato conformemente all'articolo 19, paragrafo 2.

4. Fatte salve le disposizioni relative al trattamento delle segnalazioni nel SIS contenute nei regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862 e le limitazioni necessarie per proteggere la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non saranno compromesse indagini nazionali, qualora sia creato un collegamento rosso l'autorità responsabile della verifica manuale delle identità diverse informa la persona interessata della presenza di dati di identità multipli illeciti e fornisce alla persona il numero di identificazione unico di cui all'articolo 34, lettera c), del presente regolamento, un riferimento all'autorità responsabile della verifica manuale delle identità diverse di cui all'articolo 34, lettera d), del presente regolamento, e l'indirizzo del sito web del portale in conformità dell'articolo 49 del presente regolamento.

5. L'informazione di cui al paragrafo 4 è fornita per iscritto mediante un modulo standard dall'autorità responsabile della verifica manuale delle identità diverse. La Commissione determina il contenuto e la presentazione del modulo mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

6. Qualora sia creato un collegamento rosso il MID informa in le autorità responsabili dei dati oggetto del collegamento in modo automatizzato.

7. Se l'autorità di uno Stato membro o un'agenzia dell'Unione che ha accesso al CIR o al SIS ha prove che suggeriscono che un collegamento rosso è stato erroneamente registrato nel MID o che i dati trattati nel MID, nel CIR e nel SIS sono stati trattati in violazione del presente regolamento, tale autorità o agenzia controlla i dati pertinenti registrati nel CIR e nel SIS e:

a) laddove il collegamento si riferisca a una delle segnalazioni nel SIS di cui all'articolo 29, paragrafo 2, informa l'ufficio SIRENE dello Stato membro che ha creato la segnalazione nel SIS;

b) in tutti gli altri casi, rettifica o cancella immediatamente il collegamento dal MID.

Se un ufficio SIRENE è contattato a norma del primo comma, lettera a), esso verifica le prove fornite dall'autorità dello Stato membro o dall'agenzia dell'Unione e, se del caso, rettifica o cancella immediatamente il collegamento dal MID.

L'autorità dello Stato membro che ottiene le prove informa senza indugio l'autorità dello Stato membro competente della verifica manuale delle identità diverse di ogni eventuale rettifica o cancellazione di un collegamento rosso.

Articolo 33

Collegamento bianco

1. Il collegamento tra dati di due o più sistemi di informazione dell'UE è classificato bianco nei seguenti casi:

a) il collegamento evidenzia gli stessi dati biometrici e dati di identità identici o simili;

b) il collegamento evidenzia dati di identità identici o simili, gli stessi dati relativi al documento di viaggio e almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici della persona in questione;

c) il collegamento evidenzia gli stessi dati biometrici, gli stessi dati relativi al documento di viaggio e dati di identità simili;

d) il collegamento evidenzia gli stessi dati biometrici ma dati di identità simili o differenti e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a una stessa persona in maniera giustificata.

2. Quando è interrogato il CIR o il SIS e sussiste un collegamento bianco tra i dati di due sistemi di informazione dell'UE, il MID indica che i dati di identità oggetto del collegamento si riferiscono alla stessa persona. Se l'autorità che ha avviato l'interrogazione ha accesso ai dati oggetto del collegamento in base al diritto dell'Unione o nazionale, i sistemi di informazione dell'UE interrogati rispondono indicando, se del caso, tutti i dati oggetto del collegamento riguardanti la persona, facendo così emergere una corrispondenza con i dati oggetto del collegamento bianco.

3. Qualora sia creato un collegamento bianco tra dati nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nell'ECRIS-TCN, il fascicolo individuale conservato nel CIR è aggiornato conformemente all'articolo 19, paragrafo 2.

4. Fatte salve le disposizioni relative al trattamento delle segnalazioni nel SIS contenute nei regolamenti (UE) 2018/1860, (UE) 2018/1861 and (UE) 2018/1862, e fatte salve le limitazioni necessarie per proteggere la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non siano compromesse indagini nazionali, qualora sia creato un collegamento bianco a seguito di una verifica manuale delle identità diverse, l'autorità responsabile della verifica manuale delle identità diverse informa la persona interessata della presenza di dati di identità simili o diversi e fornisce alla persona il numero di identificazione unico di cui all'articolo 34, lettera c), del presente regolamento e mette un riferimento all'autorità responsabile della verifica manuale delle identità diverse di cui all'articolo 34, lettera d), del presente regolamento e l'indirizzo del sito web del portale in conformità dell'articolo 49 del presente regolamento.

5. Se un'autorità di uno Stato membro dispone di prove indicanti che un collegamento bianco sia stato erroneamente registrato nel MID, non sia aggiornato o che i dati siano stati trattati nel MID o nei sistemi di informazione dell'UE in violazione del presente regolamento, essa controlla i dati pertinenti conservati nel CIR e nel SIS e, se necessario, rettifica o cancella senza indugio il collegamento dal MID. L'autorità dello Stato membro informa senza indugio lo Stato membro responsabile della verifica manuale delle identità diverse.

6. L'informazione di cui al paragrafo 4 è fornita per iscritto mediante un modulo standard dall'autorità responsabile della verifica manuale delle identità diverse. La Commissione determina il contenuto e la presentazione di tale modulo mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 34

Fascicolo di conferma dell'identità

Il fascicolo di conferma dell'identità contiene i seguenti dati:

a) i collegamenti di cui agli articoli da 30 a 33;

b) un riferimento ai sistemi di informazione dell'UE in cui sono conservati i dati oggetto del collegamento;

c) un numero di identificazione unico che permette di estrarre i dati oggetto del collegamento dai corrispondenti sistemi di informazione dell'UE;

d) l'autorità responsabile della verifica manuale delle identità diverse;

e) la data della creazione del link o di un suo aggiornamento.

Articolo 35

Conservazione dei dati nel rilevatore di identità multiple

I fascicoli di conferma dell'identità e i relativi dati, compresi i collegamenti, sono conservati nel MID solo per il tempo in cui i dati oggetto del collegamento sono conservati in due o più sistemi di informazione dell'UE. Essi sono successivamente cancellati dal MID in maniera automatizzata.

Articolo 36

Registrazioni

1. eu-LISA conserva le registrazioni di tutti i trattamenti di dati nel MID. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro che ha avviato l'interrogazione;

b) la finalità dell'accesso dell'utente;

c) la data e l'ora dell'interrogazione;

d) il tipo di dati usati per avviare l'interrogazione;

e) il riferimento ai dati oggetto del collegamento;

f) lo storico del fascicolo di conferma dell'identità.

2. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tale autorità debitamente autorizzato a usare il MID. Ciascuna agenzia dell'Unione conserva le registrazioni delle interrogazioni effettuate dal proprio personale

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Qualora, tuttavia, siano necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando le procedure di monitoraggio non necessitano più delle registrazioni.

CAPO VI

Misure a sostegno dell'interoperabilità

Articolo 37

Qualità dei dati

1. Fatte salve le responsabilità degli Stati membri per quanto riguarda la qualità dei dati inseriti nei sistemi, eu-LISA istituisce procedure e meccanismi automatizzati di controllo della qualità dei dati per i dati conservati nell'EES, nel VIS, nell'ETIAS, nel SIS, nel BMS comune e nel CIR.

2. eu-LISA applica meccanismi per la valutazione della precisione del BMS comune, istituisce indicatori comuni della qualità dei dati e norme minime di qualità per conservare i dati nell'EES, nel VIS, nell'ETIAS, nel SIS, nel BMS comune e nel CIR.

Solo i dati che rispettano le norme minime di qualità possono essere inseriti nell'EES, nel VIS, nell'ETIAS, nel SIS, nel BMS comune, nel CIR e nel MID.

3. eu-LISA riferisce periodicamente agli Stati membri in merito alle procedure e ai meccanismi automatizzati di controllo della qualità dei dati e agli indicatori comuni della qualità dei dati. eu-LISA riferisce periodicamente alla Commissione in merito ai problemi incontrati e agli Stati membri interessati. Su richiesta, eu-LISA presenta tale relazione anche al Parlamento europeo e al Consiglio. Nessuna delle relazioni di cui al presente paragrafo contiene dati personali.

4. I dettagli delle procedure e dei meccanismi automatizzati di controllo della qualità dei dati, gli indicatori comuni della qualità dei dati e le norme minime di qualità per conservare i dati nell'EES, nel VIS, nell'ETIAS, nel SIS, nel BMC comune e nel CIR, in particolare per quanto riguarda i dati biometrici, sono stabiliti in atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

5. Un anno dopo l'istituzione delle procedure e dei meccanismi automatizzati di controllo della qualità dei dati, degli indicatori comuni della qualità dei dati e delle norme minime di qualità dei dati, e successivamente ogni anno, la Commissione valuta l'attuazione da parte degli Stati membri dei requisiti di qualità dei dati e formula le eventuali raccomandazioni necessarie. Gli Stati membri presentano alla Commissione un piano d'azione volto a correggere le carenze riscontrate nella relazione di valutazione e, in particolare, i problemi relativi alla qualità dei dati derivanti da dati errati nei sistemi di informazione dell'UE. Gli Stati membri riferiscono regolarmente alla Commissione sui progressi compiuti con il piano d'azione fino alla sua completa attuazione.

La Commissione trasmette la relazione di valutazione al Parlamento europeo, al Consiglio, al garante europeo della protezione dei dati, al Comitato europeo per la protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali istituita con regolamento (CE) n. 168/2007 del Consiglio ([39]).

Articolo 38

Formato universale dei messaggi

1. È istituito lo standard del formato universale dei messaggi (UMF). Lo standard UMF definisce le norme relative a determinati elementi relativi al contenuto dello scambio di informazioni transfrontaliero tra i sistemi di informazione, le autorità o le organizzazioni del settore Giustizia e affari interni.

2. Lo standard UMF è usato per lo sviluppo dell'EES, dell'ETIAS, dell'ESP, del CIR, del MID e, se del caso, per lo sviluppo da parte di eu-LISA o di altra agenzia dell'UE di nuovi modelli per lo scambio di informazioni o nuovi sistemi di informazione del settore Giustizia e affari interni.

3. Ai fini dell'istituzione e dello sviluppo dello standard UMF di cui al paragrafo 1 del presente articolo, la Commissione adotta un atto di esecuzione. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 39

Archivio centrale di relazioni e statistiche

1. È istituito un archivio centrale di relazioni e statistiche (CRRS) al fine di sostenere gli obiettivi dell'EES, del VIS, dell'ETIAS e del SIS, in conformità dei pertinenti strumenti giuridici che governano tali sistemi, e fornire dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati.

2. eu-LISA istituisce, attua e ospita nei suoi siti tecnici il CRRS contenenti, separati per logica dal sistema di informazione UE, i dati e le statistiche di cui all'articolo 63 del regolamento (UE) 2017/2226, all'articolo 17 del regolamento (CE) n. 767/2008, all'articolo 84 del regolamento (UE) 2018/1240, all'articolo 60 del regolamento (UE) 2018/1861 e all'articolo 16 del regolamento (UE) 2018/1860. L'accesso al CRRS è concesso mediante un accesso controllato, sicuro e specifici profili di utente, unicamente ai fini dell'elaborazione di relazioni e statistiche, alle autorità di cui all'articolo 63 del regolamento (UE) 2017/2226, all'articolo 17 del regolamento (CE) n. 767/2008, all'articolo 84 del regolamento (UE) 2018/1240 e all'articolo 60 del regolamento (UE) 2018/1861.

3. eu-LISA anonimizza i dati e registra i dati anonimizzati nel CRRS. Il processo di anonimizzazione dei dati è automatizzato.

I dati contenuti nel CRRS non consentono l'identificazione delle persone fisiche.

4. Il CRRS è composto di:

a) strumenti necessari per anonimizzare i dati;

b) un'infrastruttura centrale, costituita da un archivio di dati anonimi;

c) un'infrastruttura di comunicazione sicura per collegare il CRRS all'EES, al VIS, all'ETIAS e al SIS, nonché alle infrastrutture centrali del BMS comune, del CIR e del MID.

5. La Commissione adotta un atto delegato conformemente all'articolo 73 per stabilire le modalità di funzionamento del CRRS, comprese le garanzie specifiche per il trattamento dei dati personali a norma dei paragrafi 2 e 3 del presente articolo e le norme di sicurezza applicabili all'archivio.

([39]) Regolamento (CE) n. 168/2007 del Consiglio, del 15 febbraio 2007, che istituisce l'Agenzia dell'Unione europea per i diritti fondamentali (GU L 53 del 22.2.2007, pag. 1).

CAPO VII

Protezione dei dati

Articolo 40

Titolare del trattamento

1. Per quanto riguarda il trattamento dei dati nel BMS comune, le autorità degli Stati membri titolari del trattamento per l'EES, il VIS e il SIS, rispettivamente, sono titolari del trattamento ai sensi dell'articolo 4, punto 7), del regolamento (UE) 2016/679 o dell'articolo 3, punto 8), della direttiva 2016/680/UE in relazione ai template biometrici ottenuti dai dati di cui all'articolo 13 del presente regolamento inseriti da ciascuna autorità nel sistema sottostante e hanno la responsabilità del trattamento dei template biometrici nel BMS comune.

2. Per quanto riguarda il trattamento dei dati nel CIR, le autorità degli Stati membri titolari del trattamento per l'EES, il VIS e l'ETIAS, rispettivamente, sono titolari del trattamento ai sensi dell'articolo 4, punto 7), del regolamento (UE) 2016/679 in relazione ai dati di cui all'articolo 18 del presente regolamento inseriti da ciascuna autorità nel sistema sottostante e hanno la responsabilità del trattamento di tali dati personali nel CIR.

3. Per quanto riguarda il trattamento dei dati nel MID:

a) l'Agenzia europea della guardia di frontiera e costiera è responsabile del trattamento ai sensi dell'articolo 3, punto 8), del regolamento (CE) n. 2018/1725 in relazione al trattamento di dati personali da parte dell'unità centrale ETIAS;

b) le autorità degli Stati membri che aggiungono o modificano dati nel fascicolo di conferma dell'identità sono titolari del trattamento ai sensi dell'articolo 4, punto 7), del regolamento (UE) 2016/679 o dell'articolo 3, punto 8), della direttiva 2016/680/UE e hanno la responsabilità del trattamento dei dati personali nel MID.

4. Per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, i titolari del trattamento hanno accesso alle registrazioni di cui agli articoli 10, 16, 24 e 36 per la verifica interna di cui all'articolo 44.

Articolo 41

Responsabile del trattamento

Per quanto riguarda il trattamento dei dati personali nel BMS comune, nel CIR e nel MID, eu-LISA è incaricato del trattamento ai sensi dell'articolo 3, punto 12), lettera a), del regolamento (UE) 2018/1725.

Articolo 42

Sicurezza del trattamento

1. eu-LISA, l'unità centrale ETIAS, Europol e le autorità degli Stati membri garantiscono la sicurezza del trattamento di dati personali svolto a norma del presente regolamento. eu-LISA, l'unità centrale ETIAS, Europol e le autorità degli Stati membri cooperano nei compiti relativi alla sicurezza.

2. Fatto salvo l'articolo 33 del regolamento (UE) 2018/1725, eu-LISA adotta le misure necessarie per garantire la sicurezza delle componenti dell'interoperabilità e delle relative infrastrutture di comunicazione.

3. In particolare 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, al fine di:

a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani d'emergenza per la protezione delle infrastrutture critiche;

b) negare alle persone non autorizzate l'accesso alle attrezzature e alle strutture utilizzate per il trattamento di dati;

c) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate;

d) impedire che i dati siano inseriti senza autorizzazione e che i dati personali registrati siano visionati, modificati o cancellati senza autorizzazione;

e) impedire che i dati siano trattati, copiati, modificati o cancellati senza autorizzazione;

f) impedire che persone non autorizzate usino sistemi di trattamento automatizzato di dati servendosi di attrezzature per la comunicazione di dati;

g) garantire che le persone autorizzate ad accedere alle componenti dell'interoperabilità abbiano accesso solo ai dati previsti dalla loro autorizzazione di accesso, tramite identità di utente individuali ed esclusivamente con modalità di accesso riservato;

h) garantire che sia possibile verificare e stabilire a quali organismi possono essere trasmessi dati personali mediante apparecchiature di comunicazione dei dati;

i) garantire che sia possibile verificare e stabilire quali dati sono stati trattati nelle componenti dell'interoperabilità, quando, da chi e per quale finalità;

j) impedire, in particolare mediante tecniche appropriate di cifratura, che, all'atto della trasmissione di dati personali dalle componenti dell'interoperabilità o verso le medesime ovvero durante il trasporto dei supporti di dati, tali dati personali vengano letti, copiati, modificati o cancellati senza autorizzazione;

k) provvedere affinché, in caso di interruzione, i sistemi installati possano essere ripristinati;

l) garantire l'affidabilità, accertandosi che eventuali anomalie nel funzionamento delle componenti dell'interoperabilità siano adeguatamente segnalate;

m) 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 e valutare le misure di sicurezza alla luce dei nuovi sviluppi tecnologici.

4. Gli Stati membri, Europol e l'unità centrale ETIAS adottano misure equivalenti a quelle del paragrafo 3 per quanto riguarda la sicurezza del trattamento dei dati personali da parte delle autorità con diritto di accesso a una o più componenti dell'interoperabilità.

Articolo 43

Incidenti di sicurezza

1. È considerato incidente di sicurezza l'evento che ha o può avere ripercussioni sulla sicurezza delle componenti dell'interoperabilità e può causare danni o perdite ai dati ivi conservati, in particolare quando possono essere stati consultati dati senza autorizzazione o quando sono state o possono essere state compromesse la disponibilità, l'integrità e la riservatezza dei dati.

2. Ogni incidente di sicurezza è gestito in modo 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, dell'articolo 30 della direttiva (UE) 2016/680, o di entrambi, gli Stati membri notificano senza indugio qualsiasi incidente di sicurezza alla Commissione, a eu-LISA, alle autorità di controllo competenti e al garante europeo della protezione dei dati

Fatti salvi gli articoli 34 e 35 del regolamento (UE) 2018/1725 e l'articolo 34 del regolamento (UE) 2016/794, l'unità centrale ETIAS ed Europol notificano senza indugio qualsiasi incidente di sicurezza alla Commissione, a eu-LISA e al garante europeo della protezione dei dati.

Qualora si verifichi un incidente di sicurezza in relazione all'infrastruttura centrale delle componenti dell'interoperabilità, eu-LISA notifica senza indugio alla Commissione e al garante europeo della protezione dei dati.

4. Le informazioni sull'incidente di sicurezza che ha o può avere ripercussioni sul funzionamento delle componenti dell'interoperabilità o sulla disponibilità, integrità e riservatezza dei dati sono fornite senza indugio agli Stati membri, all'unità centrale ETIAS e a Europol e registrate secondo il piano di gestione degli incidenti stabilito da eu-LISA.

5. Gli Stati membri interessati, l'unità centrale ETIAS, Europol ed eu-LISA cooperano in caso di incidente di sicurezza. La Commissione stabilisce con atti di esecuzione le modalità di tale procedura di cooperazione. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 74, paragrafo 2.

Articolo 44

Verifica interna

Gli Stati membri e le pertinenti agenzie dell'Unione provvedono affinché ciascuna autorità con diritto di accesso alle componenti dell'interoperabilità adotti le misure necessarie per verificare la propria conformità al presente regolamento e cooperi, se necessario, con l'autorità di controllo.

I titolari del trattamento di cui all'articolo 40 adottano le misure necessarie per verificare la conformità del trattamento di dati a norma del presente regolamento, anche attraverso la verifica frequente delle registrazioni di cui agli articoli 10, 16, 24 e 36, e cooperare, laddove necessario, con le autorità di controllo e con il garante europeo della protezione dei dati.

Articolo 45

Sanzioni

Gli Stati membri provvedono affinché qualsiasi uso improprio, trattamento o scambio di dati in contrasto con il presente regolamento sia punibile ai sensi del diritto nazionale. Le sanzioni previste sono effettive, proporzionate e dissuasive.

Articolo 46

Responsabilità

1. Fatti salvi il diritto al risarcimento e la responsabilità da parte del titolare del trattamento o del responsabile del trattamento ai sensi del regolamento (UE) 2016/679, della direttiva (UE) 2016/680 e del regolamento (UE) 2018/1725:

a) ogni persona o Stato membro che abbia subito danni materiali o immateriali in conseguenza di un trattamento illecito di dati personali 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;

b) ogni persona o Stato membro che abbia subito danni materiali o immateriali in conseguenza di qualsiasi atto incompatibile con il presente regolamento compiuto da Europol, dall'Agenzia europea della guardia di frontiera e costiera o da eu-LISA, ha diritto al risarcimento da parte dell'agenzia in questione.

Lo Stato membro interessato, Europol, l'Agenzia europea della guardia di frontiera e costiera o eu-LISA sono esonerati, in tutto o in parte, dalla responsabilità a norma del primo comma se provano che l'evento dannoso non è loro imputabile.

2. Uno Stato membro è responsabile di ogni eventuale danno arrecato alle componenti dell'interoperabilità conseguente all'inosservanza degli obblighi del presente regolamento, a meno che e nella misura in cui eu-LISA o un altro Stato membro vincolato al presente regolamento abbia omesso di adottare provvedimenti ragionevolmente idonei a prevenire il danno o ridurne al minimo l'impatto.

3. Le azioni proposte nei confronti di uno Stato membro per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono disciplinate dal diritto nazionale dello Stato membro convenuto. Le azioni proposte nei confronti del titolare del trattamento o eu-LISA per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono soggette alle condizioni previste dai trattati.

Articolo 47

Diritto di informazione

1. L'autorità che raccoglie i dati personali da conservare nel BMS comune, nel CIR o nel MID fornisce alle persone i cui dati sono raccolti con le informazioni di cui agli articoli 13 e 14 del regolamento (UE) 2016/679, agli articoli 12 e 13 della direttiva (UE) 2016/680 e agli articoli 15 e 16 del regolamento (UE) 2018/1725. L'autorità fornisce le informazioni al momento della raccolta di tali dati.

2. Tutte le informazioni sono messe a disposizione usando un linguaggio semplice e chiaro, in una versione linguistica che la persona interessata capisca o che dovrebbe ragionevolmente capire. Ciò comprende la comunicazione di informazioni in modo consono all'età dei minori interessati.

3. Le persone i cui dati sono registrati nell'EES, nel VIS o nell'ETIAS sono informate del trattamento dei dati personali ai fini del presente regolamento conformemente al paragrafo 1 quando:

a) è creato o aggiornato un fascicolo relativo alla domanda nell'EES conformemente all'articolo 14 del regolamento (UE) 2017/2226;

b) è creato o aggiornato un fascicolo relativo alla domanda nel VIS conformemente all'articolo 8 del regolamento (CE) n. 767/2008;

c) è creato o aggiornato un fascicolo relativo alla domanda nell'ETIAS conformemente all'articolo 19 del regolamento (UE) 2018/1240;

Articolo 48

Diritto di accesso ai dati personali, di rettifica e di cancellazione degli stessi conservati nel MID e limitazione del loro trattamento

1. Per esercitare i diritti di cui agli articoli da 15 a 18 del regolamento (UE) 2016/679, agli articoli da 17 a 20 del regolamento (UE) 2018/1725 e agli articoli 14, 15 e 16 della direttiva (UE) 2016/680, l'interessato ha il diritto di rivolgersi all'autorità competente di qualsiasi Stato membro, che esamina la richiesta e vi risponde.

2. Lo Stato membro che esamina la richiesta risponde senza indebito ritardo e in ogni caso entro 45 giorni dalla ricezione della richiesta. Tale termine può essere prorogato di 15 giorni, se necessario, tenuto conto della complessità e del numero delle richieste. Lo Stato membro che esamina la richiesta informa l'interessato di tale proroga, e dei motivi del ritardo, entro 45 giorni dal ricevimento della richiesta. Gli Stati membri possono stabilire che tali risposte siano fornite da uffici centrali.

3. Qualora la richiesta di rettifica o cancellazione dei dati personali sia presentata a uno Stato membro diverso da quello competente per la verifica manuale delle identità diverse, lo Stato membro al quale è stata presentata contatta le autorità dello Stato membro competente per la verifica manuale delle identità diverse entro sette giorni. Lo Stato membro competente per la verifica manuale delle identità diverse verifica senza indebito ritardo, in ogni caso entro 30 giorni da tale contatto, l'esattezza dei dati e la liceità del loro trattamento. Tale termine può essere prorogato di 15 giorni, se necessario, tenuto conto della complessità e del numero delle richieste. Lo Stato membro competente per la verifica manuale delle identità diverse informa lo Stato membro che l'ha contattato in merito a tale proroga unitamente ai motivi del ritardo. L'interessato è informato dallo Stato membro che ha contattato l'autorità dello Stato membro competente per la verifica manuale delle identità diverse in merito al prosieguo della procedura.

4. Qualora la richiesta di rettifica o cancellazione dei dati personali sia presentata a uno Stato membro in cui l'unità centrale ETIAS sia competente per la verifica manuale delle identità diverse, lo Stato membro al quale è stata presentata la richiesta contatta entro 7 giorni l'unità centrale ETIAS per chiedere un suo parere. L'unità centrale ETIAS esprime il suo parere senza indebito ritardo e in ogni caso entro 30 giorni dal momento in cui è stato contattato. Tale termine può essere prorogato di 15 giorni, se necessario, tenuto conto della complessità e del numero delle richieste. L'interessato è informato dallo Stato membro che ha contattato l'unità centrale ETIAS in merito al prosieguo della procedura.

5. Qualora da un esame emerga che i dati conservati nel MID sono inesatti o sono stati registrati illecitamente, lo Stato membro competente per la verifica manuale delle identità diverse o, ove non vi sia uno Stato membro competente per la verifica manuale delle identità diverse o qualora l'unità centrale ETIAS sia responsabile della verifica manuale delle identità diverse, lo Stato membro al quale è stata presentata la richiesta provvede a rettificare o cancellare tali dati senza indebito ritardo. L'interessato è informato per iscritto che i suoi dati sono stati rettificati o cancellati.

6. Qualora i dati conservati nel MID siano modificati da uno Stato membro durante il loro periodo di conservazione, tale Stato membro effettua il trattamento di cui all'articolo 27 e, se del caso, all'articolo 29 per determinare se i dati modificati debbano essere oggetto di un collegamento. Qualora dal trattamento non risulti alcuna corrispondenza, tale Stato membro cancella i dati dal fascicolo di conferma dell'identità. Qualora dal trattamento automatizzato risultino uno o più corrispondenze, tale Stato membro crea o aggiorna il relativo collegamento conformemente alle disposizioni pertinenti del presente regolamento.

7. Qualora non ritenga che i dati conservati nel MID siano inesatti o siano stati registrati illecitamente, lo Stato membro competente per la verifica manuale delle identità diverse o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta adotta una decisione amministrativa con la quale illustra per iscritto senza indugio all'interessato la ragione per cui non intende rettificare o cancellare i dati che lo riguardano.

8. La decisione di cui al paragrafo 7 fornisce all'interessato informazioni sulla possibilità di impugnare la decisione adottata sulla richiesta di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali e, se del caso, informazioni su come intentare un'azione o presentare un reclamo dinanzi alle autorità competenti o alle autorità giurisdizionali competenti e su qualunque tipo di assistenza, anche da parte delle autorità di controllo.

9. La richiesta di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali contiene le informazioni necessarie per identificare l'interessato. Tali informazioni sono utilizzate unicamente per consentire l'esercizio dei diritti di cui al presente articolo e sono cancellate subito dopo.

10. Lo Stato membro competente per la verifica manuale delle identità diverse o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta conserva una registrazione scritta della presentazione di una richiesta di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali e di come è stata trattata e mette senza indugio tale registrazione a disposizione delle autorità di controllo.

11. Il presente articolo lascia impregiudicate le limitazioni e le restrizioni riguardo ai diritti di cui al presente articolo ai sensi del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680.

Articolo 49

Portale web

1. È istituito un portale web allo scopo di facilitare l'esercizio dei diritti di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali.

2. Il portale web contiene informazioni sui diritti e sulle procedure di cui agli articoli 47 e 48 e un'interfaccia utente che consente alle persone i cui dati sono trattati nel MID e che sono state informate della presenza di un collegamento rosso ai sensi dell'articolo 32, paragrafo 4, di ricevere le informazioni di contatto dell'autorità competente dello Stato membro competente per la verifica manuale delle identità diverse.

3. Per ottenere le informazioni di contatto dell'autorità competente dello Stato membro responsabile della verifica manuale delle identità diverse, la persona i cui dati sono trattati nel MID dovrebbe inserire il riferimento all'autorità responsabile della verifica manuale delle identità diverse di cui all'articolo 34, lettera d). Il portale web utilizza tale riferimento per estrarre le informazioni di contatto dell'autorità competente dello Stato membro responsabile della verifica manuale delle diverse identità. Il portale web comprende anche un modello di posta elettronica per facilitare la comunicazione tra l'utente del portale e l'autorità competente dello Stato membro responsabile della verifica manuale delle identità diverse. Tale indirizzo di posta elettronica include un campo per il numero di identificazione unico di cui all'articolo 34, lettera c), per consentire all'autorità competente dello Stato membro responsabile della verifica manuale di identità diverse di identificare i dati in questione.

4. Gli Stati membri forniscono a eu-LISA i dettagli di contatto di tutte le autorità competenti a esaminare e rispondere alle richieste di cui agli articoli 47 e 48 e verificano periodicamente se tali dettagli di contatto sono aggiornati.

5. eu-LISA sviluppa il portale web e ne garantisce la gestione tecnica.

6. La Commissione adotta un atto delegato conformemente all'articolo 73 che stabilisce norme dettagliate sul funzionamento del portale web, compresa l'interfaccia utente, le lingue in cui il portale è disponibile e il modello di posta elettronica.

Articolo 50

Comunicazione di dati personali a paesi terzi, organizzazioni internazionali e soggetti privati

Fatti salvi l'articolo 65 del regolamento (UE) 2018/1240, gli articoli 25 e 26 del regolamento (UE) 2016/794, l'articolo 41 del regolamento (UE) 2017/2226, l'articolo 31 del regolamento (CE) n. 767/2008 e la consultazione delle banche dati Interpol attraverso l'ESP in conformità dell'articolo 9, paragrafo 5, del presente regolamento, che sono conformi alle disposizioni del capo V del regolamento (UE) 2018/1725 e del capo V del regolamento (UE) 2016/679, i dati personali conservati nelle componenti dell'interoperabilità o da queste trattati o consultati non sono trasferiti o messi a disposizione di paesi terzi, organizzazioni internazionali o soggetti privati.

Articolo 51

Controllo delle autorità di controllo

1. Ciascuno Stato membro assicura che le autorità di controllo monitorino indipendentemente la legittimità del trattamento dei dati personali a norma del presente regolamento da parte dello Stato membro interessato, compresa la loro trasmissione alle componenti dell'interoperabilità e viceversa.

2. Ciascuno Stato membro provvede affinché le disposizioni legislative, regolamentari e amministrative nazionali adottate ai sensi della direttiva (UE) 2016/680 siano altresì applicabili, ove necessario, in merito all'accesso alle componenti dell'interoperabilità da parte delle autorità di polizia e delle autorità designate, anche per quanto riguarda i diritti delle persone i cui dati sono così consultati.

3. Le autorità di controllo provvedono affinché, almeno ogni quattro anni, sia svolto un audit dei trattamenti di dati personali da parte delle autorità nazionali competenti ai fini del presente regolamento conformemente ai pertinenti principi internazionali di audit.

Le autorità di controllo pubblicano ogni anno il numero delle richieste di rettifica, cancellazione o limitazione del trattamento dei dati personali, le conseguenti azioni intraprese e il numero delle rettifiche, cancellazioni e limitazioni del trattamento effettuate in seguito alle richieste degli interessati.

4. Gli Stati membri provvedono affinché le proprie autorità di controllo dispongano delle risorse e delle competenze sufficienti per assolvere i compiti loro assegnati dal presente regolamento.

5. Gli Stati membri comunicano qualsiasi informazione richiesta da un'autorità di controllo di cui all'articolo 51, paragrafo 1, del regolamento (UE) 2016/679 e, in particolare, le forniscono informazioni sulle attività svolte conformemente alle loro responsabilità ai sensi del presente regolamento. Gli Stati membri consentono alle autorità di controllo di cui all'articolo 51, paragrafo 1, del regolamento (UE) 2016/679 di accedere alle loro registrazioni di cui agli articoli 10, 16, 24 e 36 del presente regolamento, di accedere alle giustificazioni di cui all'articolo 22, paragrafo 2, del presente regolamento, e di accedere in qualsiasi momento a tutti i loro locali utilizzati ai fini dell'interoperabilità.

Articolo 52

Audit del garante europeo della protezione dei dati

Il garante europeo della protezione dei dati provvede affinché almeno ogni quattro anni sia svolto un audit delle operazioni di trattamento dei dati personali effettuate da eu-LISA, dall'unità centrale ETIAS e da Europol ai fini del presente regolamento conformemente ai pertinenti principi internazionali di audit. Una relazione su tale audit è trasmessa al Parlamento europeo, al Consiglio, a eu-LISA, alla Commissione, agli Stati membri e all'agenzia dell'Unione interessata. A eu-LISA, all'unità centrale ETIAS e a Europol è data la possibilità di presentare osservazioni prima dell'adozione della relazione.

eu-LISA, l'unità centrale ETIAS e Europol forniscono al garante europeo della protezione dei dati le informazioni da questo richieste, consentono al garante europeo della protezione dei dati di accedere a tutti i documenti e alle loro registrazioni di cui agli articoli 10, 16, 24 e 36 e gli consentono di accedere in qualsiasi momento a tutti i loro locali.

Articolo 53

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 nell'ambito delle rispettive responsabilità e assicurano il controllo coordinato dell'uso delle componenti dell'interoperabilità e dell'applicazione delle altre disposizioni del presente regolamento, in particolare se il garante europeo della protezione dei dati o un'autorità di controllo constata notevoli differenze tra le pratiche degli Stati membri o trasferimenti potenzialmente illeciti nell'uso dei canali di comunicazione delle componenti dell'interoperabilità.

2. Nei casi di cui al paragrafo 1 del presente articolo, è assicurato il controllo coordinato a norma dell'articolo 62 del regolamento (UE) 2018/1725.

3. Entro il 12 giugno 2021 e, successivamente, ogni due anni, il comitato europeo per la protezione dei dati trasmette al Parlamento europeo, al Consiglio, alla Commissione, a Europol, all'Agenzia europea della guardia di frontiera e costiera e a eu-LISA una relazione congiunta sulle sue attività ai sensi del presente articolo. Tale relazione comprende un capitolo su ciascuno Stato membro redatto dall'autorità di controllo dello Stato membro interessato.

CAPO XIII

Responsabilità

Articolo 54

Responsabilità di eu-LISA in fase di progettazione e sviluppo

1. eu-LISA garantisce che le infrastrutture centrali delle componenti dell'interoperabilità siano gestite conformemente al presente regolamento.

2. Le componenti dell'interoperabilità sono ospitate da eu-LISA nei suoi siti tecnici e forniscono le funzionalità di cui al presente regolamento nel rispetto delle condizioni di sicurezza, disponibilità, qualità e prestazione di cui all'articolo 55, paragrafo 1.

3. eu-LISA è responsabile dello sviluppo delle componenti dell'interoperabilità e di ogni adattamento necessario per istituire l'interoperabilità tra i sistemi centrali dell'EES, del VIS, dell'ETIAS, del SIS, dell'Eurodac, dell'ECRIS-TCN dell'ESP, del BMS comune, del CIR, del MID e del CRRS.

Fatto salvo l'articolo 66, eu-LISA non ha accesso a nessuno dei dati personali trattati attraverso l'ESP, il BMS comune, il CIR o il MID.

eu-LISA definisce la progettazione dell'architettura fisica delle componenti dell'interoperabilità, comprese le rispettive infrastrutture di comunicazione, e le specifiche tecniche e la loro evoluzione per quanto riguarda l'infrastruttura centrale e l'infrastruttura di comunicazione sicura, che sono adottate dal consiglio di amministrazione previo parere favorevole della Commissione. eu-LISA provvede anche agli adattamenti dell'EES, del VIS, dell'ETIAS o del SIS resi necessari dall'interoperabilità e previsti dal presente regolamento.

eu-LISA sviluppa e implementa le componenti dell'interoperabilità non appena possibile dopo l'entrata in vigore del presente regolamento e l'adozione da parte della Commissione delle misure di cui all'articolo 8, paragrafo 2, all'articolo 9, paragrafo 7, all'articolo 28, paragrafi 5 e 7, all'articolo 37, paragrafo 4, all'articolo 38, paragrafo 3, all'articolo 39, paragrafo 5, all'articolo 43, paragrafo 5, e all'articolo 78, paragrafo 10.

Lo sviluppo comporta l'elaborazione e l'applicazione delle specifiche tecniche, il collaudo e la gestione e il coordinamento generale del progetto.

4. In fase di progettazione e di sviluppo, è istituito un consiglio di gestione del programma composto di un massimo di 10 membri. Esso è costituito da sette membri nominati dal consiglio di amministrazione di eu-LISA tra i suoi membri o i supplenti, dal presidente del gruppo consultivo sull'interoperabilità di cui all'articolo 75, da un membro che rappresenta eu-LISA nominato dal suo direttore esecutivo e da un membro nominato dalla Commissione. I membri nominati dal consiglio di amministrazione di eu-LISA sono eletti soltanto tra detti Stati membri che sono pienamente vincolati, in base al diritto dell'Unione, dagli strumenti giuridici che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi di informazione dell'UE e che partecipano alle componenti dell'interoperabilità.

5. Il consiglio di gestione del programma si riunisce periodicamente, almeno tre volte a trimestre. Esso garantisce l'adeguata gestione della fase di progettazione e sviluppo delle componenti dell'interoperabilità.

Ogni mese il consiglio di gestione del programma presenta relazioni scritte al consiglio di amministrazione di eu-LISA sui progressi del progetto. Il consiglio di gestione del programma non ha potere decisionale, né mandato di rappresentare i membri del consiglio di amministrazione di eu-LISA.

6. Il consiglio di amministrazione di eu-LISA stabilisce il regolamento interno del consiglio di gestione del programma, che comprende in particolare disposizioni concernenti:

a) la presidenza;

b) i luoghi di riunione;

c) la preparazione delle riunioni;

d) l'ammissione di esperti alle riunioni;

e) i piani di comunicazione atti a garantire che siano fornite informazioni complete ai membri non partecipanti del consiglio di amministrazione.

La presidenza è esercitata da uno Stato membro che è pienamente vincolato, in base al diritto dell'Unione, dagli strumenti giuridici che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi di informazione dell'UE e che parteciperanno ai componenti dell'interoperabilità.

Tutte le spese di viaggio e di soggiorno sostenute dai membri del consiglio di gestione del programma sono a carico di eu-LISA e l'articolo 10 del suo regolamento interno si applica mutatis mutandis. eu-LISA fornisce un segretariato al consiglio di gestione del programma.

Il gruppo consultivo sull'interoperabilità di cui all'articolo 75 si riunisce regolarmente fino all'entrata in funzione delle componenti dell'interoperabilità. Dopo ciascuna riunione, riferisce al consiglio di gestione del programma. Fornisce la consulenza tecnica a sostegno delle attività del consiglio di gestione del programma e monitora lo stato di preparazione degli Stati membri.

Articolo 55

Responsabilità di eu-LISA in seguito all'entrata in funzione

1. In seguito all'entrata in funzione di ciascuna componente dell'interoperabilità, eu-LISA è responsabile della gestione tecnica dell'infrastruttura centrale delle componenti dell'interoperabilità, compresi la loro manutenzione e gli sviluppi tecnologici. In cooperazione con gli Stati membri, provvede a che siano utilizzate, previa analisi costi/benefici, le migliori tecnologie disponibili. eu-LISA è inoltre responsabile della gestione tecnica dell'infrastruttura di comunicazione di cui agli articoli 6, 12, 17, 25 e 39.

La gestione tecnica delle componenti dell'interoperabilità consiste nell'insieme dei compiti e delle soluzioni tecniche necessari per garantire il funzionamento delle componenti dell'interoperabilità e fornendo ininterrottamente servizi agli Stati membri e alle agenzie dell'Unione 24 ore su 24 e 7 giorni su 7 in conformità del presente regolamento e comprende, in particolare, la manutenzione e gli adeguamenti tecnici necessari per garantire che le componenti funzionino a un livello di qualità tecnica soddisfacente, specialmente per quanto riguarda i tempi di risposta alle interrogazioni dell'infrastruttura centrale, conformemente alle specifiche tecniche.

Tutte le componenti dell'interoperabilità sono sviluppate e gestite in modo tale da garantire una disponibilità rapida, continuata, efficiente e un accesso controllato, pieno e ininterrotto delle componenti e dei dati conservati nel MID, nel BMS comune e nel CIR, e un tempo di risposta in linea con le esigenze operative delle autorità degli Stati membri e delle agenzie dell'Unione.

2. Fatto salvo l'articolo 17 dello statuto dei funzionari dell'Unione europea, eu-LISA applica ai membri del proprio personale che operano con i dati conservati nelle componenti dell'interoperabilità adeguate norme in materia di segreto professionale o altri obblighi di riservatezza equivalenti. Tale obbligo vincola il personale anche dopo che ha lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

Fatto salvo l'articolo 66, eu-LISA non ha accesso a nessuno dei dati personali trattati attraverso l'ESP, il BMS comune, il CIR e il MID.

3. eu-LISA sviluppa e mantiene un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati conservati nel BMS comune e nel CIR conformemente all'articolo 37.

4. eu-LISA svolge compiti relativi alla formazione sull'uso tecnico delle componenti dell'interoperabilità.

Articolo 56

Responsabilità degli Stati membri

1. Ciascuno Stato membro è responsabile di quanto segue:

a) la connessione all'infrastruttura di comunicazione dell'ESP e del CIR;

b) l'integrazione dei sistemi e delle infrastrutture nazionali esistenti con l'ESP, il CIR e il MID;

c) l'organizzazione, la gestione, il funzionamento e la manutenzione della propria infrastruttura nazionale esistente e della sua connessione alle componenti dell'interoperabilità;

d) la gestione e le modalità di accesso all'ESP, al CIR e al MID del personale debitamente autorizzato delle autorità nazionali competenti, quale che sia il tipo di autorizzazione, a norma del presente regolamento, nonché la creazione e l'aggiornamento periodico di un elenco di tale personale con le relative qualifiche;

e) l'adozione delle misure legislative di cui all'articolo 20, paragrafi 5 e 6, ai fini dell'accesso al CIR a fini di identificazione;

f) la verifica manuale delle identità diverse di cui all'articolo 29;

g) la conformità ai requisiti di qualità dei dati stabiliti dal diritto dell'Unione;

h) la conformità alle norme di ciascun sistema di informazione dell'UE riguardanti la sicurezza e l'integrità dei dati personali;

i) la correzione delle carenze riscontrate nella relazione di valutazione della Commissione riguardante la qualità dei dati di cui all'articolo 37, paragrafo 5.

2. Ciascuno Stato membro provvede alla connessione delle rispettive autorità designate al CIR.

Articolo 57

Responsabilità dell'unità centrale ETIAS

L'unità centrale ETIAS è responsabile di quanto segue:

a) la verifica manuale delle identità diverse a norma dell'articolo 29;

b) la rilevazione di identità multiple tra i dati conservati nell'EES, nel VIS, nell'Eurodac e nel SIS di cui all'articolo 69.

CAPO IX

Modifiche di altri strumenti dell'Unione

Articolo 58

Modifiche del regolamento (CE) n. 767/2008

Il regolamento (CE) n. 767/2008 è così modificato:

1) all'articolo 1 è aggiunto il comma seguente:

«Conservando nell'archivio comune di dati di identità (CIR) istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/817 (*) i dati di identità, i dati del documento di viaggio e i dati biometrici, il VIS concorre ad agevolare e contribuire alla corretta identificazione delle persone registrate nel VIS alle condizioni e per gli obiettivi dell'articolo 20 di tale regolamento.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE settore nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).»;

2) all'articolo 4 sono aggiunti i punti seguenti:

«12) "dati del VIS", tutti i dati conservati nel sistema centrale VIS e nel CIR conformemente agli articoli da 9 a 14;

13) "dati di identità", i dati di cui all'articolo 9, punto 4), lettere a) e a *bis*);

14) "dati relativi alle impronte digitali", i dati relativi alle cinque impronte digitali del dito indice, medio, anulare, mignolo e pollice della mano destra e, se disponibili, della mano sinistra;»;

3) all'articolo 5 è inserito il paragrafo seguente:

«1 *bis*. Il CIR contiene i dati di cui all'articolo 9, punto 4), lettere da a) a c), e punti 5 e 6. I rimanenti dati del VIS sono conservati nel sistema centrale VIS.»;

4) all'articolo 6 il paragrafo 2 è sostituito dal seguente:

«2. L'accesso al VIS per la consultazione dei dati è riservato esclusivamente al personale debitamente autorizzato delle autorità nazionali di ciascuno Stato membro competenti per gli scopi definiti agli articoli da 15 a 22 e al personale debitamente autorizzato delle autorità nazionali di ciascuno Stato membro e delle agenzie dell'Unione che sono competenti per gli scopi di cui agli articoli 20 e 21 del regolamento (UE) 2019/817. Tale accesso è limitato conformemente alla misura in cui i dati siano necessari all'assolvimento dei propri compiti per detti scopi e siano proporzionati agli obiettivi perseguiti.»;

5) all'articolo 9, punto 4), le lettere da a) a c) sono sostituite dalle seguenti:

«a) cognome; nome/i; data di nascita; sesso;

a *bis*) cognome alla nascita (precedente/i cognome/i); luogo e paese di nascita; attuale cittadinanza e cittadinanza alla nascita;

b) tipo e numero del documento o dei documenti di viaggio e codice a tre lettere del paese di rilascio del documento o dei documenti di viaggio;

c) data di scadenza del documento o dei documenti di viaggio;

c *bis*) autorità che ha rilasciato il documento di viaggio e data di rilascio;».

Articolo 59

Modifiche del regolamento (UE) 2016/399

All'articolo 8 è inserito il paragrafo seguente:

«4 *bis*. Se, all'ingresso o all'uscita, la consultazione delle banche dati pertinenti, compreso il rilevatore di identità multiple attraverso il portale di ricerca europeo istituito dall'articolo 25, paragrafo 1, e dall'articolo 6, paragrafo 1, del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio (*) dà luogo, rispettivamente, a un collegamento giallo o rileva un collegamento rosso, la guardia di frontiera consulta l'archivio comune di dati di identità istituito dall'articolo 17, paragrafo 1, di tale regolamento o il SIS, o entrambi, al fine di valutare le differenze tra i dati di identità o i dati dei documenti di viaggio oggetto del collegamento. La guardia di frontiera effettua le verifiche aggiuntive necessarie per decidere sullo status e sul colore del collegamento.

Conformemente all'articolo 69, paragrafo 1, del regolamento (UE) 2019/817, il presente paragrafo si applica esclusivamente a partire dall'entrata in funzione del rilevatore di identità multiple ai sensi dell'articolo 72, paragrafo 4, di tale regolamento.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE settore nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).».

Articolo 60

Modifiche del regolamento (UE) 2017/2226

Il regolamento (UE) 2017/2226 è così modificato:

1) all'articolo 1, è aggiunto il paragrafo seguente:

«3. Conservando nell'archivio comune di dati di identità (CIR) istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio (*) i dati di identità, i dati del documento di viaggio e i dati biometrici, l'EES concorre ad agevolare e contribuire alla corretta identificazione delle persone registrate nell'EES alle condizioni e per gli obiettivi dell'articolo 20 di tale regolamento.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE settore nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).»;

2) all'articolo 3, il paragrafo 1 è così modificato:

a) il punto 22) è sostituito dal seguente:

«22) "dati dell'EES", tutti i dati conservati nel sistema centrale dell'EES e nel CIR conformemente agli articoli da 15 a 20;»;

b) è inserito il punto seguente:

«22 *bis*) "dati di identità": i dati di cui all'articolo 16, paragrafo 1, lettera a), nonché i dati pertinenti di cui all'articolo 17, paragrafo 1, e all'articolo 18, paragrafo 1;»;

c) sono aggiunti i punti seguenti:

«32) "ESP": il portale di ricerca europeo istituito dall'articolo 6, paragrafo 1, del regolamento (UE) 2019/817»;

33) "CIR": l'archivio comune di dati di identità istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/817;»;

3) all'articolo 6, paragrafo 1, è aggiunta la lettera seguente:

«j) garantire la corretta identificazione delle persone.»;

4) l'articolo 7 è così modificato:

a) il paragrafo 1 è cosi modificato:

i) è inserita la lettera seguente:

«a *bis*) l'infrastruttura centrale del CIR di cui all'articolo 17, paragrafo 2, lettera a), del regolamento (UE) 2019/817;»;

ii) la lettera f) è sostituita dalla seguente:

«f) un'infrastruttura di comunicazione sicura tra il sistema centrale dell'EES e le infrastrutture centrali dell'ESP e del CIR.»;

b) è inserito il paragrafo seguente:

«1 *bis*. Il CIR contiene i dati di cui all'articolo 16, paragrafo 1, lettere da a) a d), all'articolo 17, paragrafo 1, lettere a), b) e c), e all'articolo 18, paragrafi 1 e 2. I rimanenti dati dell'EES sono conservati nel sistema centrale dell'EES.»;

5) all'articolo 9, è aggiunto il paragrafo seguente:

«4. L'accesso ai dati dell'EES conservati nel CIR è riservato esclusivamente al personale debitamente autorizzato delle autorità nazionali di ciascuno Stato membro e al personale debitamente autorizzato delle agenzie dell'Unione che sono competenti per gli scopi di cui agli articoli 20 e 21 del regolamento (UE) 2019/817. Tale accesso è limitato conformemente alla misura in cui i dati siano necessari all'assolvimento dei propri compiti per tali scopi, ed è proporzionato agli obiettivi perseguiti.»;

6) l'articolo 21 è cosi modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. Qualora sia tecnicamente impossibile inserire i dati nel sistema centrale dell'EES o nel CIR, o in caso di guasto del sistema centrale dell'EES o del CIR, i dati di cui agli articoli da16 a 20 sono temporaneamente conservati nella NUI. Qualora ciò non sia possibile, i dati sono temporaneamente conservati localmente in un formato elettronico. In entrambi i casi, i dati sono inseriti nel sistema centrale dell'EES o nel CIR non appena l'impossibilità tecnica o il guasto siano stati risolti. Gli Stati membri adottano le opportune misure e mobilitano le infrastrutture, le attrezzature e le risorse necessarie per garantire che tale conservazione locale temporanea possa essere effettuata in qualsiasi momento e per qualsiasi loro valico di frontiera.»;

b) al paragrafo 2, il primo comma è sostituito dal seguente:

«2. Fatto salvo l'obbligo di procedere alle verifiche di frontiera ai sensi del regolamento (UE) 2016/399, nel caso eccezionale in cui sia tecnicamente impossibile inserire i dati sia nel sistema centrale dell'EES che nel CIR che nella NUI e sia tecnicamente impossibile conservare temporaneamente i dati localmente in un formato elettronico, l'autorità di frontiera conserva manualmente i dati di cui agli articoli da 16 a 20 del presente regolamento a eccezione dei dati biometrici, e appone un timbro d'ingresso o di uscita sul documento di viaggio del cittadino di paese terzo. Tali dati sono inseriti nel sistema centrale dell'EES e nel CIR non appena tecnicamente possibile.»;

7) l'articolo 23 è cosi modificato:

a) è inserito il paragrafo seguente:

«2 *bis*. Ai fini delle verifiche a norma del paragrafo 1 del presente articolo, l'autorità di frontiera avvia un'interrogazione utilizzando l'ESP per confrontare i dati sui cittadini di paesi terzi con i dati pertinenti nell'EES e nel VIS.»;

b) al paragrafo 4 il primo comma è sostituito dal seguente:

«4. Qualora dall'interrogazione con i dati alfanumerici di cui al paragrafo 2 del presente articolo risulti che i dati relativi al cittadino di paese terzo non sono registrati nell'EES, se una verifica del cittadino di paese terzo a norma del paragrafo 2 del presente articolo non dà esito o se sussistono dubbi quanto all'identità del cittadino di paese terzo, le autorità di frontiera hanno accesso ai dati a fini di identificazione conformemente all'articolo 27, al fine di creare o aggiornare un fascicolo individuale ai sensi dell'articolo 14.»;

8) all'articolo 32 è inserito il paragrafo seguente:

«1 *bis*. Le autorità designate possono accedere all'EES a fini di consultazione qualora, in caso di interrogazione del CIR avviata conformemente all'articolo 22 del regolamento (UE) 2019/817, le condizioni stabilite dal presente articolo sono soddisfatte e la risposta ricevuta di cui all'articolo 22, paragrafo 2, del regolamento (UE) 2019/817 indichi che nell'EES sono conservati dati.»;

9) all'articolo 33 è inserito il paragrafo seguente:

«1 *bis*. Europol può accedere all'EES a fini di consultazione qualora, in caso di interrogazione del CIR avviata conformemente all'articolo 22 del regolamento (UE) 2019/817, le condizioni stabilite dal presente articolo sono soddisfatte e la risposta di cui all'articolo 22, paragrafo 2, del regolamento (UE) 2019/817 indichi che nell'EES sono conservati dati.»;

10) l'articolo 34 è così modificato:

a) ai paragrafi 1 e 2, i termini «nel sistema centrale dell'EES» sono sostituiti dai termini «nel CIR e nel sistema centrale dell'EES»;

b) al paragrafo 5, i termini «dal sistema centrale dell'EES» sono sostituiti dai termini «dal sistema centrale dell'EES e dal CIR»;

11) all'articolo 35, il paragrafo 7 è sostituito dal seguente:

«7. Il sistema centrale dell'EES e il CIR informano immediatamente tutti gli Stati membri della cancellazione dei dati dell'EES o del CIR e, ove applicabile, li eliminano dall'elenco di persone identificate di cui all'articolo 12, paragrafo 3.»;

12) all'articolo 36, i termini «del sistema centrale dell'EES» sono sostituiti dai termini «del sistema centrale dell'EES e del CIR»;

13) l'articolo 37 è così modificato:

a) il primo comma del paragrafo 1 è sostituito dal seguente:

«1. eu-LISA è responsabile dello sviluppo del sistema centrale dell'EES, del CIR, delle NUI, dell'infrastruttura di comunicazione e del canale di comunicazione sicuro tra il sistema centrale dell'EES e il sistema centrale del VIS. eu-LISA è inoltre responsabile dello sviluppo del servizio web di cui all'articolo 13 secondo le norme dettagliate di cui all'articolo 13, paragrafo 7, e secondo le specifiche e le condizioni adottate conformemente all'articolo 36, primo comma, lettera h), e dello sviluppo dell'archivio di dati di cui all'articolo 63, paragrafo 2.»;

b) al paragrafo 3 il primo comma è sostituito dal seguente:

«3. eu-LISA è responsabile della gestione operativa del sistema centrale dell'EES, del CIR, delle NUI e del canale di comunicazione sicuro tra il sistema centrale dell'EES e il sistema centrale del VIS. In cooperazione con gli Stati membri, provvede a che in qualsiasi momento siano utilizzate, previa analisi costi/benefici, le migliori tecnologie disponibili per il sistema centrale dell'EES, il CIR, le NUI, l'infrastruttura di comunicazione, il canale di comunicazione sicuro tra il sistema centrale dell'EES e il sistema centrale del VIS, il servizio web di cui all'articolo 13 e l'archivio di dati di cui all'articolo 63, paragrafo 2. eu-LISA è inoltre responsabile della gestione operativa dell'infrastruttura di comunicazione tra il sistema centrale dell'EES e le NUI, del servizio web di cui all'articolo 13 e dell'archivio di dati di cui all'articolo 63, paragrafo 2.»;

14) all'articolo 46, paragrafo 1, è aggiunta la lettera seguente:

«f) un riferimento all'uso dell'ESP per interrogare l'EES di cui all'articolo 7, paragrafo 2, del regolamento (UE) 2019/817.»;

15) l'articolo 63 è così modificato:

a) il paragrafo 2 è sostituito dal seguente:

«2. Ai fini del paragrafo 1 del presente articolo, eu-LISA conserva i dati di cui a tale paragrafo nell'archivio centrale di relazioni e statistiche di cui all'articolo 39 del regolamento (UE) 2019/817.»;

b) al paragrafo 4 è aggiunto il comma seguente:

«Le statistiche giornaliere sono conservate nell'archivio centrale di relazioni e statistiche.».

Articolo 61

Modifiche del regolamento (UE) 2018/1240

Il regolamento (UE) 2018/1240 è così modificato:

1) all'articolo 1 è aggiunto il paragrafo seguente:

«3. Conservando i dati di identità e i dati del documento di viaggio nell'archivio comune di dati di identità (CIR) istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/817 (*), ETIAS concorre ad agevolare e contribuire alla corretta identificazione delle persone registrate nell'ETIAS alle condizioni e per gli obiettivi di cui all'articolo 20 di tale regolamento.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE settore nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).»;

2) all'articolo 3, paragrafo 1, sono aggiunti i punti seguenti:

«23) "CIR": l'archivio comune di dati di identità istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/817;

24) "ESP": il portale di ricerca europeo istituito dall'articolo 6, paragrafo 1, del regolamento (UE) 2019/817;

25) "sistema centrale ETIAS": il sistema centrale di cui all'articolo 6, paragrafo 2, lettera a), unitamente al CIR, nella misura in cui questo contiene i dati di cui all'articolo 6, paragrafo 2 *bis*;

26) "dati di identità": i dati di cui all'articolo 17, paragrafo 2, lettere a) b) e c);

27) "dati del documento di viaggio": i dati di cui all'articolo 17, paragrafo 2, lettere d) ed e), e il codice a tre lettere del paese di rilascio del documento di viaggio di cui all'articolo 19, paragrafo 3, lettera c).»;

3) all'articolo 4 è aggiunta la lettera seguente:

«g) contribuisce alla corretta identificazione delle persone.»;

4) l'articolo 6 è così modificato:

a) il paragrafo 2 è così modificato:

i) la lettera a) è sostituita dalla seguente:

«a) un sistema centrale, compreso l'elenco di controllo ETIAS di cui all'articolo 34;»;

ii) è inserita la lettera seguente:

«a *bis*) il CIR;»;

iii) la lettera d) è sostituita dalla seguente:

«d) un'infrastruttura di comunicazione sicura tra il sistema centrale e le infrastrutture centrali dell'ESP e del CIR;»;

b) è inserito il paragrafo seguente:

«2 *bis*. Il CIR contiene i dati di identità e i dati del documento di viaggio. I rimanenti dati sono conservati nel sistema centrale.»;

5) l'articolo 13 è così modificato:

a) è inserito il paragrafo seguente:

«4 *bis*. L'accesso ai dati di identità e ai dati del documento di viaggio dell'ETIAS conservati nel CIR è riservato esclusivamente al personale debitamente autorizzato delle autorità nazionali di ciascuno Stato membro e al personale debitamente autorizzato delle agenzie dell'Unione che sono competenti per gli scopi di cui agli articoli 20 e 21 del regolamento (UE) 2019/817. Tale accesso è limitato conformemente alla misura in cui i dati siano necessari all'assolvimento dei propri compiti per tali scopi, e proporzionato agli obiettivi perseguiti.»;

b) il paragrafo 5 è sostituito dal seguente:

«5. Ciascuno Stato membro designa le autorità nazionali competenti di cui ai paragrafi 1, 2, 4 e 4 *bis* del presente articolo e ne comunica senza indugio a eu-LISA l'elenco, in conformità dell'articolo 87, paragrafo 2. Tale elenco specifica lo scopo per cui il personale debitamente autorizzato di ciascuna autorità ha accesso ai dati conservati nel sistema d'informazione dell'ETIAS conformemente ai paragrafi 1, 2, 4 e 4 *bis* del presente articolo.»;

6) all'articolo 17 il paragrafo 2 è così modificato:

a) la lettera a) è sostituita dalla seguente:

«a) cognome, nome o nomi, cognome alla nascita, data di nascita, luogo di nascita, sesso, attuale cittadinanza;»;

b) è inserita la lettera seguente:

«a *bis*) paese di nascita, nome o nomi dei genitori;»;

7) all'articolo 19, paragrafo 4, i termini «articolo 17, paragrafo 2, lettera a)» sono sostituiti dai termini «articolo 17, paragrafo 2, lettere a) e a *bis*)»;

8) l'articolo 20 è così modificato:

a) al paragrafo 2, il primo comma è sostituito dal seguente:

«2. Il sistema centrale ETIAS avvia un'interrogazione utilizzando l'ESP per confrontare i dati pertinenti di cui all'articolo 17, paragrafo 2, lettere a), a *bis*), b), c), d), f), g), j), k) e m), e paragrafo 8, con i dati contenuti in una cartella, un fascicolo o una segnalazione registrati in un fascicolo di domanda memorizzato nel sistema centrale ETIAS, nel SIS, nell'EES, nel VIS, nell'Eurodac, nei dati Europol, e nelle banche dati Interpol, SLTD e TDAWN.»;

b) al paragrafo 4, i termini «articolo 17, paragrafo 2, lettere a), b), c), d), f), g), j), k) e m)» sono sostituiti dai termini «articolo 17, paragrafo 2, lettere a), a *bis*), b), c), d), f), g), j), k) e m)»;

c) al paragrafo 5, i termini «articolo 17, paragrafo 2, lettere a), b), c), d), f), h) e i)» sono sostituiti dai termini «articolo 17, paragrafo 2, lettere a), a *bis*), c), f), h) e i)»;

9) all'articolo 23, il paragrafo 1 è sostituito dal seguente:

«1. Il sistema centrale ETIAS avvia un'interrogazione utilizzando l'ESP per confrontare i dati pertinenti di cui all'articolo 17, paragrafo 2, lettere a), a *bis*), b) e d), con i dati presenti nel SIS, per stabilire se il richiedente sia oggetto di una delle seguenti segnalazioni:

a) segnalazione di persona scomparsa;

b) segnalazione di persona ricercata nell'ambito di un procedimento giudiziario;

c) segnalazione di persona da sottoporre a controllo discreto o controllo specifico.»;

10) all'articolo 52 è inserito il paragrafo seguente:

«1 *bis*. Le autorità designate possono accedere a fini di consultazione ai fascicoli di domanda conservati nel sistema centrale ETIAS a norma del presente articolo qualora, in caso di interrogazione del CIR conformemente all'articolo 22 del regolamento (UE) 2019/817, la risposta ricevuta di cui all'articolo 22, paragrafo 2, del regolamento (UE) 2019/817 indichi che in detti fascicoli sono conservati dati.»;

11) all'articolo 53 è inserito il paragrafo seguente:

«1 *bis*. Europol può accedere a fini di consultazione ai fascicoli di domanda conservati nel sistema centrale ETIAS a norma del presente articolo qualora, in caso di interrogazione del CIR conformemente all'articolo 22 del regolamento (UE) 2019/817, la risposta ricevuta di cui all'articolo 22, paragrafo 2, del regolamento (UE) 2019/817 indichi che in detti fascicoli sono conservati dati.»;

12) all'articolo 65, paragrafo 3, quinto comma, i termini «articolo 17, paragrafo 2, lettere a), b), d), e) e f)» sono sostituiti dai termini «articolo 17, paragrafo 2, lettere a), a *bis*), b), d), e) e f)»;

13) all'articolo 69, paragrafo 1, è inserita la lettera seguente:

«ca) se del caso, un riferimento all'uso dell'ESP per interrogare il sistema centrale ETIAS di cui all'articolo 7, paragrafo 2, del regolamento (UE) 2019/817;»;

14) all'articolo 73, paragrafo 2, i termini «il repertorio centrale di dati» sono sostituiti dai termini «l'archivio centrale di relazioni e statistiche di cui all'articolo 39 del regolamento (UE) 2019/817, in quanto contenga dati ottenuti dal sistema centrale ETIAS conformemente all'articolo 84 del presente regolamento;»;

15) all'articolo 74, paragrafo 1, il primo comma è sostituito dal seguente;

«1. In seguito all'entrata in funzione dell'ETIAS, eu-LISA è responsabile della gestione tecnica del sistema centrale ETIAS e delle interfacce uniformi nazionali. È altresì responsabile dell'eventuale collaudo tecnico richiesto per la creazione e l'aggiornamento delle regole di esame ETIAS. In cooperazione con gli Stati membri provvede a che in qualsiasi momento siano utilizzate, previa analisi costi/benefici, le migliori tecnologie disponibili. eu-LISA è inoltre responsabile della gestione tecnica dell'infrastruttura di comunicazione tra il sistema centrale ETIAS e le IUN, nonché del sito web pubblico, dell'applicazione per dispositivi mobili, del servizio di posta elettronica, del servizio di account sicuro, dello strumento di verifica per i richiedenti, dello strumento di consenso per i richiedenti, dello strumento di valutazione per l'elenco di controllo ETIAS, del portale per i vettori, del servizio web e del software per il trattamento delle domande.»;

16) all'articolo 84, paragrafo 2, il primo comma è sostituito dal seguente:

«2. Ai fini del paragrafo 1 del presente articolo, eu-LISA conserva i dati di cui a tale paragrafo nell'archivio centrale di relazioni e statistiche di cui all'articolo 39 del regolamento (UE) 2019/817. Ai sensi dell'articolo 39, paragrafo 1, di tale regolamento, i dati statistici intersistemici e le relazioni analitiche permettono alle autorità elencate al paragrafo 1 del presente articolo di ottenere relazioni e dati statistici personalizzabili al fine di sostenere l'applicazione delle regole di screening ETIAS previste all'articolo 33, migliorare la valutazione dei rischi per la sicurezza, di immigrazione illegale e di alto rischio epidemico, migliorare l'efficienza delle verifiche di frontiera e assistere l'unità centrale ETIAS e le unità nazionali ETIAS nel trattamento delle domande di autorizzazione ai viaggi.»;

17) all'articolo 84, paragrafo 4, è aggiunto il comma seguente:

«Le statistiche giornaliere sono conservate nell'archivio centrale di relazioni e statistiche di cui all'articolo 39 del regolamento (UE) 2019/817.».

Articolo 62

Modifiche del regolamento (UE) 2018/1726

Il regolamento (UE) 2018/1726 è così modificato:

1) l'articolo 12 è sostituito dal seguente:

«*Articolo 12*

Qualità dei dati

1. Fatte salve le responsabilità degli Stati membri per quanto riguarda i dati inseriti nei sistemi sotto la responsabilità operativa dell'Agenzia, quest'ultima, in stretta collaborazione con i suoi gruppi consultivi, predispone, per tutti i sistemi di cui ha la responsabilità operativa, procedure e meccanismi automatizzati di controllo della qualità dei dati, indicatori comuni della qualità dei dati e norme minime di qualità per conservare i dati, in conformità degli strumenti giuridici che disciplinano tali sistemi d'informazione e dell'articolo 37 dei regolamenti (UE) 2019/817 (*) e (UE) 2019/818 (**) del Parlamento europeo e del Consiglio.

2. L'Agenzia istituisce un archivio centrale, contenente unicamente dati anonimizzati, di relazioni e statistiche a norma dell'articolo 39 dei regolamenti (UE) 2019/817 e (UE) 2019/818, fatte salve specifiche disposizioni contenute negli strumenti giuridici che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi IT su larga scala gestiti dall'Agenzia.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).

(**) Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85).»;

2) all'articolo 19, il paragrafo 1 è così modificato:

a) è inserita la lettera seguente:

«ee *bis*) adotta relazioni sulla situazione dello sviluppo delle componenti dell'interoperabilità a norma dell'articolo 78, paragrafo 2, del regolamento (UE) 2019/817 e dell'articolo 74, paragrafo 2, del regolamento (UE) 2019/818;»;

b) la lettera ff) è sostituita dalla seguente:

«ff) adotta relazioni sul funzionamento tecnico del SIS II in conformità dell'articolo 60, paragrafo 7, del regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio (*) e dell'articolo 74, paragrafo 8, del regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio (**), sul funzionamento tecnico del VIS in conformità dell'articolo 50, paragrafo 3, del regolamento (CE) n. 767/2008 e dell'articolo 17, paragrafo 3, della decisione 2008/633/GAI, dell'EES in conformità dell'articolo 72, paragrafo 4, del regolamento (UE) 2017/2226, dell'ETIAS in conformità dell'articolo 92, paragrafo 4, del regolamento (UE) 2018/1240, dell'ECRIS-TCN e dell'implementazione di riferimento ECRIS in conformità dell'articolo 36, paragrafo 8, del regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio (***) e sul funzionamento delle componenti dell'interoperabilità in conformità dell'articolo 78, paragrafo 3, del regolamento (UE) 2019/817 e dell'articolo 74, paragrafo 3, del regolamento (UE) 2019/818;

(*) Regolamento (UE) 2018/1861 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 (GU L 312 del 7.12.2018, pag. 14).

(**) Regolamento (UE) 2018/1862 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 della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e 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 312 del 7.12.2018, pag. 56).

(***) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1)»;

c) la lettera hh) è sostituita dalla seguente:

«hh) adotta osservazioni formali sulle relazioni del Garante europeo della protezione dei dati relative ai suoi controlli in conformità dell'articolo 56, paragrafo 2, del regolamento (UE) 2018/1861, dell'articolo 42, paragrafo 2, del regolamento (CE) n. 767/2008, dell'articolo 31, paragrafo 2, del regolamento (UE) n. 603/2013, dell'articolo 56, paragrafo 2, del regolamento (UE) 2017/2226, dell'articolo 67 del regolamento (UE) 2018/1240, dell'articolo 29, paragrafo 2, del regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio e dell'articolo 52 dei regolamenti (UE) 2019/817 e (UE) 2019/818 e assicura adeguato seguito a tali controlli;»;

d) la lettera mm) è sostituita dalla seguente:

«mm) provvede alla pubblicazione annuale dell'elenco delle autorità competenti autorizzate a consultare direttamente i dati inseriti nel SIS in conformità dell'articolo 41, paragrafo 8, del regolamento (UE) 2018/1861 e dell'articolo 56, paragrafo 7, del regolamento (UE) 2018/1862, nonché dell'elenco degli uffici dei sistemi nazionali del SIS (N.SIS) e degli uffici SIRENE di cui, rispettivamente, all'articolo 7, paragrafo 3, del regolamento (UE) 2018/1861 e all'articolo 7, paragrafo 3, del regolamento (UE) 2018/1862, come pure dell'elenco delle autorità competenti di cui all'articolo 65, paragrafo 2, del regolamento (UE) 2017/2226, dell'elenco delle autorità competenti di cui all'articolo 87, paragrafo 2, del regolamento (UE) 2018/1240, dell'elenco delle autorità centrali di cui all'articolo 34, paragrafo 2, del regolamento (UE) 2019/816 e dell'elenco delle autorità di cui all'articolo 71, paragrafo 1, del regolamento (UE) 2019/817 e dell'articolo 67, paragrafo 1, del regolamento (UE) 2019/818;»;

3) all'articolo 22, il paragrafo 4 è sostituito dal seguente:

«4. Europol e Eurojust possono assistere alle riunioni del consiglio di amministrazione in qualità di osservatori quando sono all'ordine del giorno questioni concernenti il SIS II, in relazione all'applicazione della decisione 2007/533/GAI.

L'Agenzia europea della guardia di frontiera e costiera può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore quando sono all'ordine del giorno questioni concernenti il SIS, in relazione all'applicazione del regolamento (UE) 2016/1624.

Europol può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore quando sono all'ordine del giorno questioni concernenti il VIS, in relazione all'applicazione della decisione 2008/633/GAI, o questioni concernenti l'Eurodac, in relazione all'applicazione del regolamento (UE) n. 603/2013.

Europol può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore quando sono all'ordine del giorno questioni concernenti l'EES, in relazione all'applicazione del regolamento (UE) 2017/2226, o questioni concernenti l'ETIAS, in relazione al regolamento (UE) 2018/1240.

L'Agenzia europea della guardia di frontiera e costiera può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore anche quando è all'ordine del giorno una questione concernente l'ETIAS in relazione all'applicazione del regolamento (UE) 2018/1240.

Eurojust, Europol e la Procura europea possono assistere alle riunioni del consiglio di amministrazione in qualità di osservatori quando è all'ordine del giorno una questione concernente il regolamento (UE) 2019/816.

Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera possono assistere alle riunioni del consiglio di amministrazione in qualità di osservatori quando è all'ordine del giorno una questione concernente i regolamenti (UE) 2019/817 e (UE) 2019/818.

Il consiglio di amministrazione può invitare qualsiasi altra persona, il cui parere possa essere rilevante, a presenziare alle riunioni in veste di osservatore.»;

4) all'articolo 24, paragrafo 3, la lettera p) è sostituita dalla seguente:

«p) fatto salvo l'articolo 17 dello statuto dei funzionari, stabilire le clausole di riservatezza per conformarsi all'articolo 17 del regolamento (CE) n. 1987/2006, all'articolo 17 della decisione 2007/533/GAI, all'articolo 26, paragrafo 9, del regolamento (CE) n. 767/2008, all'articolo 4, paragrafo 4, del regolamento (UE) n. 603/2013, all'articolo 37, paragrafo 4, del regolamento (UE) 2017/2226, all'articolo 74, paragrafo 2, del regolamento (UE) 2018/1240, all'articolo 11, paragrafo 16, del regolamento (UE) 2019/816 e all'articolo 55, paragrafo 2, dei regolamenti (UE) 2019/817 e (UE) 2019/818;»;

5) l'articolo 27 è così modificato:

a) al paragrafo 1, è inserita la lettera seguente:

«d *bis*) gruppo consultivo sull'interoperabilità;»;

b) il paragrafo 3 è sostituito dal seguente:

«3. Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera possono nominare un rappresentante ciascuno in seno al gruppo consultivo SIS II.

Europol può nominare un rappresentante in seno ai gruppi consultivi VIS ed Eurodac ed EES-ETIAS.

L'Agenzia europea della guardia di frontiera e costiera può nominare anche un rappresentante in seno al gruppo consultivo EES-ETIAS.

Eurojust, Europol e la Procura europea possono nominare ciascuno un rappresentante in seno al gruppo consultivo ECRIS-TCN.

Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera possono nominare un rappresentante ciascuno in seno al gruppo consultivo sull'interoperabilità.».

Articolo 63

Modifiche del regolamento (UE) 2018/1861

Il regolamento (UE) 2018/1861 è così modificato:

1) all'articolo 3 sono aggiunti i punti seguenti:

«22) "ESP": il portale di ricerca europeo istituito dall'articolo 6, paragrafo 1, del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio (*)

23) "BMS comune": il servizio comune di confronto biometrico istituito dall'articolo 12, paragrafo 1, del regolamento (UE) 2019/817;

24) "CIR": l'archivio comune di dati di identità istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/817;

25) "MID": il rilevatore di identità multiple istituito dall'articolo 25, paragrafo 1, del regolamento (UE) 2019/817.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE settore nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).»;

2) l'articolo 4 è così modificato:

a) al paragrafo 1 le lettere b) e c) sono sostituite dalle seguenti:

«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;

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 dati tra gli uffici SIRENE di cui all'articolo 7, paragrafo 2; e

d) un'infrastruttura di comunicazione sicura tra il CS-SIS e le infrastrutture centrali dell'ESP, del BMS comune e del MID.»;

b) sono aggiunti i paragrafi seguenti:

«8. Fatti salvi i paragrafi da 1 a 5, i dati SIS possono essere consultati tramite l'ESP.

9. Fatti salvi i paragrafi da 1 a 5, i dati SIS possono anche essere trasmessi tramite l'infrastruttura di comunicazione sicura di cui al paragrafo 1, lettera d). La trasmissione è limitata alla misura in cui i dati siano necessari per gli scopi del regolamento (UE) 2019/817.»;

3) all'articolo 7 è inserito il paragrafo seguente:

«2 *bis*. Gli uffici SIRENE provvedono alla verifica manuale delle identità diverse a norma dell'articolo 29 del regolamento (UE) 2019/817. Nella misura necessaria ad assolvere tale compito, gli uffici SIRENE hanno accesso ai dati conservati nel CIR e nel MID per le finalità di cui agli articoli 21 e 26 del regolamento (UE) 2019/817.»;

4) all'articolo 12, il paragrafo 1 è sostituito dal seguente:

«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).

Gli Stati membri provvedono affinché ogni accesso ai dati personali tramite l'ESP sia registrato per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati e ai fini dell'autocontrollo e dell'integrità e sicurezza dei dati.»;

5) all'articolo 34, paragrafo 1, è aggiunta la lettera seguente:

«g) della verifica delle identità diverse e del contrasto della frode di identità in conformità del capo V del regolamento (UE) 2019/817.»;

6) all'articolo 60, il paragrafo 6 è sostituito dal seguente:

«6. Ai fini dell'articolo 15, paragrafo 4, e dei paragrafi 3, 4 e 5 del presente articolo, eu-LISA memorizza nell'archivio centrale di relazioni e statistiche di cui all'articolo 39 del regolamento (UE) 2019/817 i dati di cui all'articolo 15, paragrafo 4, e al paragrafo 3 del presente articolo che non consentono l'identificazione delle persone fisiche.

eu-LISA permette alla Commissione e agli organismi di cui paragrafo 5 del presente articolo di ottenere relazioni e statistiche personalizzate. Su richiesta, eu-LISA concede agli Stati membri, alla Commissione, a Europol e all'Agenzia europea della guardia di frontiera e costiera l'accesso all'archivio centrale di relazioni e statistiche in conformità dell'articolo 39 del regolamento (UE) 2019/817.».

Articolo 64

Modifiche della decisione 2004/512/CE

All'articolo 1 della decisione 2004/512/CE il paragrafo 2 è sostituito dal seguente:

«2. Il sistema di informazione visti è basato su un'architettura centralizzata ed è costituito da:

a) l'infrastruttura centrale del CIR di cui all'articolo 17, paragrafo 2, lettera a), del regolamento (UE) 2019/817 (*)

b) un sistema d'informazione centrale, in seguito denominato "sistema centrale di informazione visti" o "CS-VIS";

c) un'interfaccia in ciascuno Stato membro, in seguito denominata "interfaccia nazionale" o "NI-VIS", per assicurare il collegamento con la competente autorità centrale nazionale del rispettivo Stato membro;

d) un'infrastruttura di comunicazione tra il sistema centrale di informazione visti e le interfacce nazionali;

e) un canale di comunicazione sicuro fra il sistema centrale dell'EES e il CS-VIS;

f) un'infrastruttura di comunicazione sicura tra il sistema centrale VIS e le infrastrutture centrali del portale di ricerca europeo istituito dall'articolo 6, paragrafo 1, del regolamento (UE) 2019/817 e dell'archivio comune di dati di identità istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/817.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE settore nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).».

Articolo 65

Modifiche della decisione 2008/633/GAI

La decisione 2008/633/CE è così modificata:

1) all'articolo 5, è inserito il paragrafo seguente:

«1 *bis*. Le autorità designate possono accedere al VIS a fini di consultazione qualora, in caso di interrogazione dell'archivio comune di dati di identità (CIR) conformemente all'articolo 22 del regolamento (UE) 2019/817 (*) ed essendo rispettate le condizioni di accesso di cui al presente articolo, la risposta di cui all'articolo 22, paragrafo 2, di tale regolamento indichi che nel VIS sono conservati dati.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE settore nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).»;

2) all'articolo 7 è inserito il paragrafo seguente:

«1 *bis*. Europol può accedere al VIS a fini di consultazione qualora, in caso di interrogazione del CIR conformemente all'articolo 22 del regolamento (UE) 2019/817 ed essendo rispettate le condizioni di accesso di cui al presente articolo, la risposta ricevuta di cui all'articolo 22, paragrafo 2, di tale regolamento indichi che nel VIS sono conservati dati.».

CAPO X

Disposizioni finali

Articolo 66

Comunicazione e valutazione

1. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi all'ESP, unicamente per elaborare relazioni e statistiche:

a) numero di interrogazioni per utente del profilo ESP;

b) numero di interrogazioni di ciascuna banca dati Interpol.

Non è possibile identificare individualmente i dati.

2. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi al CIR, unicamente per elaborare relazioni e statistiche:

a) numero di interrogazioni ai fini degli articoli 20, 21 e 22;

b) cittadinanza, genere e anno di nascita della persona interessata;

c) tipo del documento di viaggio e codice a tre lettere del paese di rilascio;

d) numero di interrogazioni effettuate con dati biometrici e senza.

Non è possibile identificare individualmente i dati.

3. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi al MID, unicamente per elaborare relazioni e statistiche:

a) numero di interrogazioni effettuate con dati biometrici e senza;

b) numero di ciascun tipo di collegamento e i sistemi di informazione dell'UE contenenti i dati di collegamento;

c) periodo di tempo in cui un collegamento giallo e rosso è rimasto nel sistema.

Non è possibile identificare individualmente i dati.

4. Il personale debitamente autorizzato dell'Agenzia europea della guardia di frontiera e costiera ha accesso alla consultazione dei dati di cui ai paragrafi 1, 2 e 3 del presente articolo ai fini dell'esecuzione delle analisi del rischio e delle valutazioni delle vulnerabilità di cui agli articoli 11 e 13 del regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio ([40]).

5. Il personale debitamente autorizzato di Europol ha accesso alla consultazione dei dati di cui ai paragrafi 2 e 3 del presente articolo ai fini dell'esecuzione delle analisi strategiche, tematiche e operative di cui all'articolo 18, paragrafo 2, lettere b) e c), del regolamento (UE) 2016/794.

6. Ai fini dei paragrafi l, 2 e 3, eu-LISA conserva i dati di cui a tali paragrafi nel CRRS. Non è possibile identificare persone fisiche dai dati inclusi nel CRRS ma i dati permettono alle autorità di cui ai paragrafi l, 2 e 3 di ricavare relazioni e dati statistici personalizzabili al fine di migliorare l'efficienza delle verifiche di frontiera, assistere le autorità nel trattamento delle domande di visto e sostenere politiche migratorie dell'Unione basate su dati concreti.

7. Su richiesta, la Commissione mette a disposizione dell'Agenzia dell'Unione europea per i diritti fondamentali le informazioni pertinenti al fine di valutare l'impatto del presente regolamento sui diritti fondamentali.

Articolo 67

Periodo transitorio per l'uso del portale di ricerca europeo

1. Per un periodo di due anni a decorrere dall'entrata in funzione del portale di ricerca europeo gli obblighi di cui all'articolo 7, paragrafi 2 e 4, non si applicano e l'uso del portale è facoltativo.

2. Alla Commissione è conferito il potere di adottare un atto delegato conformemente all'articolo 73 per modificare il presente regolamento prorogando una volta il termine di cui al paragrafo 1 del presente articolo di non oltre un anno, qualora una valutazione dell'attuazione dell'ESP abbia dimostrato che tale proroga è necessaria, in particolare in vista dell'impatto dell'entrata in funzione dell'ESP sull'organizzazione e sulla lunghezza delle verifiche di frontiera.

Articolo 68

Periodo transitorio per l'applicazione delle disposizioni sull'accesso all'archivio comune di dati di identità a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi

L'articolo 22, l'articolo 60, punti 8 e 9, l'articolo 61, punti 10 e 11, e l'articolo 65 si applicano a decorrere dalla data di entrata in funzione del CIR di cui all'articolo 72, paragrafo 3.

([40]) 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).

Articolo 69

Periodo transitorio per il rilevatore di identità multiple

1. Per un periodo di un anno dopo che eu-LISA comunica il completamento del collaudo del MID di cui all'articolo 72, paragrafo 4, lettera b), e prima dell'entrata in funzione di quest'ultimo, l'unità centrale ETIAS è competente per effettuare le rilevazioni di identità multiple usando i dati conservati nell'EES, nel VIS, nell'Eurodac e nel SIS. Le rilevazioni di identità multiple sono effettuate usando esclusivamente i dati biometrici.

2. Qualora dall'interrogazione risultino uno o più riscontri positivi e i dati di identità nei fascicoli oggetto del collegamento siano identici o simili, è creato un collegamento bianco conformemente all'articolo 33.

Qualora dall'interrogazione risultino uno o più riscontri positivi e i dati di identità nei fascicoli oggetto del collegamento non possano essere considerati simili, è creato un collegamento giallo conformemente all'articolo 30 e si applica la procedura di cui all'articolo 29.

Qualora risultino più riscontri positivi è creato un collegamento tra tutti i dati per i quali è emerso un riscontro positivo.

3. Qualora sia creato un collegamento giallo il MID permette all'unità centrale ETIAS di consultare i dati di identità presenti nei vari sistemi di informazione dell'UE.

4. Qualora sia creato un collegamento con una segnalazione nel SIS diversa da una segnalazione a norma dell'articolo 3 del regolamento (UE) 2018/1860, degli articoli 24 e 25 del regolamento (UE) 2018/1861 o dell'articolo 38 del regolamento (UE) 2018/1862, il MID permette all'ufficio SIRENE dello Stato membro che ha creato la segnalazione di consultare i dati di identità presenti nei vari sistemi di informazione.

5. L'unità centrale ETIAS o, nei casi di cui al paragrafo 4 del presente articolo, l'ufficio SIRENE dello Stato membro che ha creato la segnalazione accede ai dati contenuti nel fascicolo di conferma dell'identità ed esamina le identità diverse, aggiorna il collegamento conformemente agli articoli 31, 32 e 33 e lo aggiunge al fascicolo di conferma dell'identità.

6. L'unità centrale ETIAS comunica alla Commissione le informazioni di cui all'articolo 71, paragrafo 3, solo dopo che tutti i collegamenti gialli siano stati verificati manualmente e il loro status sia stato aggiornato come collegamento verde, bianco o rosso.

7. Se necessario gli Stati membri forniscono assistenza all'unità centrale ETIAS ai fini dello svolgimento delle rilevazioni di identità multiple a norma del presente articolo.

8. Alla Commissione è conferito il potere di adottare un atto delegato conformemente all'articolo 73 per modificare il presente regolamento prorogando il termine di cui al paragrafo 1 del presente articolo di sei mesi, rinnovabile due volte per sei mesi alla volta. Tale proroga è concessa unicamente a seguito di una valutazione del tempo stimato per completare le rilevazioni di identità multiple a norma del presente articolo, che la rilevazione di identità multiple non possa essere completata prima dello scadere del periodo rimanente a norma del paragrafo 1 del presente articolo o di una proroga in corso, per motivi indipendenti dall'unità centrale ETIAS, e che non sia possibile applicare misure correttive. Tale valutazione è effettuata entro tre mesi prima della scadenza di tale periodo o di una proroga in corso.

Articolo 70

Spese

1. Le spese sostenute per l'istituzione e il funzionamento dell'ESP, del BMS comune, del CIR e del MID sono a carico del bilancio dell'Unione.

2. Le spese sostenute per l'integrazione delle esistenti infrastrutture nazionali e la loro connessione alle interfacce nazionali uniformi nonché per ospitare le interfacce nazionali uniformi sono a carico del bilancio generale dell'Unione.

Sono escluse le seguenti spese:

a) l'ufficio di gestione di progetto degli Stati membri (riunioni, missioni, uffici);

b) l'hosting dei sistemi IT nazionali (spazio, implementazione, elettricità, impianti di raffreddamento);

c) la gestione di sistemi IT nazionali (operatori e contratti di assistenza);

d) la progettazione, lo sviluppo, l'implementazione, il funzionamento e la manutenzione di reti di comunicazione nazionali.

3. Fatti salvi gli ulteriori finanziamenti a tal fine da altre fonti del bilancio generale dell'Unione europea, un importo di 32 077 000 EUR è mobilitato dalla dotazione di 791 000 000 EUR prevista a norma dell'articolo 5, paragrafo 5, lettera b), del regolamento (UE) n. 515/2014 per coprire i costi di attuazione del presente regolamento, come previsto ai paragrafi 1 e 2 del presente articolo.

4. Dalla dotazione di cui al paragrafo 3, 22 861 000 EUR sono assegnati a eu-LISA, 9 072 000 EUR sono assegnati a Europol e 144 000 EUR sono assegnati all'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL), per sostenere tali agenzie nell'espletamento dei rispettivi compiti conformemente al presente regolamento. Tali finanziamenti sono attuati in regime di gestione indiretta.

5. Le spese sostenute dalle autorità designate sono a carico degli Stati membri designanti. Le spese per connettere al CIR ciascuna autorità designata sono a carico di ciascuno Stato membro.

Le spese sostenute da Europol, comprese quelle per connettersi al CIR, sono sostenute da Europol.

Articolo 71

Comunicazioni

1. Gli Stati membri comunicano a eu-LISA i nominativi delle rispettive autorità di cui agli articoli 7, 20, 21 e 26 che possono usare l'ESP, il CIR e il MID o accedervi.

Entro tre mesi dall'entrata in funzione di ciascuna componente dell'interoperabilità a norma dell'articolo 72, un elenco consolidato di tali autorità è pubblicato nella *Gazzetta ufficiale dell'Unione europea*. Qualora l'elenco subisca modifiche, eu-LISA pubblica una volta all'anno un elenco consolidato aggiornato.

2. eu-LISA comunica alla Commissione il positivo completamento del collaudo di cui all'articolo 72, paragrafo 1, lettera b), al paragrafo 2 lettera b), al paragrafo 3, lettera b), al paragrafo 4, lettera b), al paragrafo 5, lettera b), e al paragrafo 6, lettera b).

3. L'unità centrale ETIAS comunica alla Commissione il positivo completamento del periodo transitorio di cui all'articolo 69.

4. La Commissione mette a disposizione degli Stati membri e del pubblico le informazioni notificate ai sensi del paragrafo 1, tenendo costantemente aggiornata la pagina web.

Articolo 72

Inizio delle attività

1. La Commissione determina la data a partire dalla quale l'ESP entra in funzione mediante un atto di esecuzione una volta che siano soddisfatte le seguenti condizioni:

a) siano state adottate le misure di cui all'articolo 8, paragrafo 2, all'articolo 9, paragrafo 7, e all'articolo 43, paragrafo 5;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale dell'ESP che deve essere effettuato in cooperazione con le autorità degli Stati membri e le agenzie dell'Unione che potrebbero utilizzare l'ESP;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 8, paragrafo 1, e le abbia comunicate alla Commissione.

L'ESP consulta le banche dati Interpol solo se le disposizioni tecniche consentono di rispettare l'articolo 9, paragrafo 5. L'eventuale impossibilità di rispettare l'articolo 9, paragrafo 5, comporta la mancata consultazione delle banche dati Interpol da parte dell'ESP, ma non ritarda l'avvio delle attività dell'ESP.

La Commissione fissa la data di cui al primo comma entro 30 giorni dall'adozione dell'atto di esecuzione.

2. La Commissione determina la data a partire dalla quale il BMS comune entra in funzione mediante un atto di esecuzione una volta che siano soddisfatte le seguenti condizioni:

a) siano state adottate le misure di cui all'articolo 13, paragrafo 5, e all'articolo 43, paragrafo 5;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del BMS comune che deve essere effettuato in cooperazione con le autorità degli Stati membri;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 13, e le abbia comunicate alla Commissione;

d) eu-LISA abbia dichiarato il positivo completamento del collaudo di cui al paragrafo 5, lettera b).

La Commissione fissa la data di cui al primo comma entro 30 giorni dall'adozione dell'atto di esecuzione.

3. La Commissione fissa la data a partire dalla quale il CIR entra in funzione mediante un atto di esecuzione una volta che siano soddisfatte le seguenti condizioni:

a) siano state adottate le misure di cui all'articolo 43, paragrafo 5, e all'articolo 78, paragrafo 10;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del CIR che è effettuato in cooperazione con le autorità degli Stati membri;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 18 e le abbia comunicate alla Commissione;

d) eu-LISA abbia dichiarato il positivo completamento del collaudo di cui al paragrafo 5, lettera b).

La Commissione fissa la data di cui al primo comma entro 30 giorni dall'adozione dell'atto di esecuzione.

4. La Commissione determina la data a partire dalla quale il MID entra in funzione mediante un atto di esecuzione una volta che siano soddisfatte le seguenti condizioni:

a) siano state adottate le misure di cui all'articolo 28, paragrafi 5 e 7, all'articolo 32, paragrafo 5, all'articolo 33, paragrafo 6, all'articolo 43, paragrafo 5, e all'articolo 49, paragrafo 6;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del MID, che è effettuato in cooperazione con le autorità degli Stati membri e l'unità centrale ETIAS;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 34 e le abbia comunicate alla Commissione;

d) l'unità centrale ETIAS abbia comunicato alla Commissione le informazioni conformemente all'articolo 71, paragrafo 3;

e) eu-LISA abbia dichiarato il positivo completamento del collaudo di cui al paragrafo 1, lettera b), al paragrafo 2, lettera b), al paragrafo 3, lettera b), e al paragrafo 5, lettera b).

La Commissione fissa la data di cui al primo comma entro 30 giorni dall'adozione dell'atto di esecuzione.

5. La Commissione determina, con atti di esecuzione, la data a partire dalla quale i meccanismi e le procedure di controllo automatico della qualità dei dati, gli indicatori comuni per la qualità dei dati e le norme minime di qualità sui dati devono essere utilizzati una volta che siano soddisfatte le seguenti condizioni:

a) siano state adottate le misure di cui all'articolo 37, paragrafo 4;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale dei meccanismi e delle procedure di controllo automatico della qualità dei dati, degli indicatori comuni per la qualità dei dati e delle norme minime di qualità dei dati, che ha effettuato in cooperazione con le autorità degli Stati membri.

La Commissione fissa la data di cui al primo comma entro 30 giorni dall'atto di esecuzione.

6. La Commissione determina la data a partire dalla quale il CRRS entra in funzione mediante un atto di esecuzione una volta che siano soddisfatte le seguenti condizioni:

a) siano state adottate le misure di cui all'articolo 39, paragrafo 5, e all'articolo 43, paragrafo 5;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del CRRS che ha effettuato in cooperazione con le autorità degli Stati membri;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 39 e le abbia comunicate alla Commissione.

La Commissione fissa la data di cui al primo comma entro 30 giorni dall'adozione dell'atto di esecuzione.

7. La Commissione informa il Parlamento europeo e il Consiglio dell'esito dei collaudi effettuati a norma del paragrafo 1, lettera b), del paragrafo 2, lettera b), del paragrafo 3, lettera b), del paragrafo 4, lettera b), del paragrafo 5, lettera b), e del paragrafo 6, lettera b).

8. Gli Stati membri, l'unità centrale ETIAS ed Europol iniziano a utilizzare ciascuna delle componenti dell'interoperabilità a decorrere dalla data stabilita dalla Commissione ai sensi, rispettivamente, dei paragrafi 1, 2, 3 e 4.

Articolo 73

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 28, paragrafo 5, all'articolo 39, paragrafo 5, all'articolo 49, paragrafo 6, all'articolo 67, paragrafo 2, e all'articolo 69, paragrafo 8, è conferito alla Commissione per un periodo di cinque anni a decorrere dall'11 giugno 2019. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega dei poteri di cui all'articolo 28, paragrafo 5, all'articolo 39, paragrafo 5, all'articolo 49, paragrafo 6, all'articolo 67, paragrafo 2, e all'articolo 69, paragrafo 8, 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 28, paragrafo 5, dell'articolo 39, paragrafo 5, dell'articolo 49, paragrafo 6, dell'articolo 67, paragrafo 2, e dell'articolo 69, paragrafo 8, 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 74

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.

Qualora il comitato non esprima alcun parere, la Commissione non adotta il progetto di atto di esecuzione e si applica l'articolo 5, paragrafo 4, terzo comma, del regolamento (UE) n. 182/2011.

Articolo 75

Gruppo consultivo

eu-LISA istituisce un gruppo consultivo sull'interoperabilità. In fase di progettazione e di sviluppo delle componenti dell'interoperabilità si applica l'articolo 54, paragrafi 4, 5 e 6.

Articolo 76

Formazione

eu-LISA svolge compiti relativi all'offerta di formazione sull'uso tecnico delle componenti dell'interoperabilità a norma del regolamento (UE) 2018/1726.

Le autorità degli Stati membri e le agenzie dell'Unione forniscono al loro personale autorizzato a trattare i dati utilizzando le componenti dell'interoperabilità adeguati programmi di formazione sulla sicurezza dei dati, la qualità dei dati, le norme in materia di protezione dei dati, le procedure applicabili al trattamento dei dati e gli obblighi d'informazione conformemente agli articoli 32, paragrafo 4, 33, paragrafo 4, e 47.

Se del caso, sono organizzati corsi di formazione congiunti a livello dell'Unione per rafforzare la cooperazione e lo scambio di migliori pratiche tra il personale delle autorità degli Stati membri e delle agenzie dell'Unione autorizzate a trattare i dati utilizzando le componenti dell'interoperabilità. È prestata particolare attenzione al processo di individuazione multipla dell'identità, compresa la verifica manuale delle identità diverse e la relativa necessità di mantenere idonee garanzie dei diritti fondamentali.

Articolo 77

Manuale pratico

La Commissione, in stretta cooperazione con gli Stati membri, eu-LISA e altre agenzie pertinenti, dell'Unione mette a disposizione un manuale pratico per l'implementazione e la gestione delle componenti dell'interoperabilità. Il manuale pratico fornisce orientamenti tecnici e operativi, raccomandazioni e migliori prassi. La Commissione adotta il manuale pratico sotto forma di raccomandazione.

Articolo 78

Monitoraggio e valutazione

1. eu-LISA provvede affinché siano istituite procedure per monitorare lo sviluppo delle componenti dell'interoperabilità e la loro connessione all'interfaccia uniforme nazionale rispetto agli obiettivi relativi alla pianificazione e ai costi, nonché per monitorare il funzionamento delle componenti dell'interoperabilità rispetto agli obiettivi prefissati in termini di risultati tecnici, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

2. Entro il 12 dicembre 2019 e successivamente ogni sei mesi durante la fase di sviluppo delle componenti, eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sulla situazione dello sviluppo delle componenti dell'interoperabilità nonché sulla loro connessione all'interfaccia uniforme nazionale. Una volta che lo sviluppo è completato, è presentata al Parlamento europeo e al Consiglio una relazione che illustra nel dettaglio il modo in cui sono stati conseguiti gli obiettivi, in particolare quelli relativi alla pianificazione e ai costi, giustificando eventuali scostamenti.

3. Quattro anni dopo l'entrata in funzione di ciascuna componente dell'interoperabilità in conformità dell'articolo 72, e successivamente ogni quattro anni, eu-LISA presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico delle componenti dell'interoperabilità, compresa la loro sicurezza.

4. Un anno dopo ogni relazione di eu-LISA la Commissione effettua una valutazione globale delle componenti di interoperabilità, che comprende:

a) una valutazione dell'applicazione del presente regolamento;

b) un'analisi dei risultati conseguiti in relazione agli obiettivi del presente regolamento e della sua incidenza sui diritti fondamentali, compresa in particolare una valutazione dell'impatto delle componenti dell'interoperabilità sul diritto alla non discriminazione;

c) una valutazione del funzionamento del portale web, compresi dati relativi all'utilizzo del portale web e il numero di richieste risolte;

d) una valutazione della perdurante validità dei principi di base delle componenti dell'interoperabilità;

e) una valutazione della sicurezza delle componenti dell'interoperabilità;

f) una valutazione dell'uso del CIR a fini di identificazione;

g) una valutazione dell'uso del CIR a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi;

h) una valutazione delle eventuali implicazioni, incluso qualsiasi impatto sproporzionato sul flusso di traffico ai valichi di frontiera, e di quelle aventi un impatto sul bilancio generale dell'Unione;

i) una valutazione della ricerca nelle banche dati Interpol attraverso l'ESP che comprenda informazioni sul numero di riscontri ottenuti dalle banche dati Interpol e informazioni sugli eventuali problemi riscontrati.

La valutazione complessiva a norma del primo comma del presente paragrafo comprende le necessarie raccomandazioni. La Commissione trasmette la relazione di valutazione al Parlamento europeo, al Consiglio, al garante europeo della protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali.

5. Entro il 12 giugno 2020 e successivamente ogni anno fino all'adozione degli atti di esecuzione della Commissione di cui all'articolo 72, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sullo stato di avanzamento dei preparativi per la piena attuazione del presente regolamento. Tale relazione contiene anche informazioni particolareggiate sulle spese sostenute e sugli eventuali rischi che possono incidere sui costi complessivi.

6. Due anni dopo l'entrata in funzione del MID in conformità dell'articolo 72, paragrafo 4, la Commissione effettua un esame dell'impatto del MID sul diritto alla non discriminazione. In seguito a questa prima relazione, l'esame dell'impatto del MID sul diritto alla non discriminazione deve far parte dell'esame di cui al paragrafo 4, lettera b), del presente articolo.

7. Gli Stati membri ed Europol comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi da 3 a 6. Tali informazioni non mettono a repentaglio i metodi di lavoro né comprendono indicazioni sulle fonti, sui membri del personale o sulle indagini delle autorità designate.

8. eu-LISA comunica alla Commissione le informazioni necessarie per redigere la valutazione complessiva di cui al paragrafo 4.

9. Nel rispetto delle disposizioni del diritto nazionale relative alla pubblicazione di informazioni sensibili, e fatte salve le limitazioni necessarie per tutelare la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non sia compromessa alcuna indagine nazionale, ciascuno Stato membro ed Europol predispongono relazioni annuali sull'efficacia dell'accesso ai dati conservati nel CIR a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, in cui figurino informazioni e statistiche su quanto segue:

a) gli scopi esatti delle consultazioni, compresi i tipi di reati di terrorismo o altri reati gravi;

b) i fondati motivi addotti per un sospetto fondato che l'autore presunto o effettivo oppure la vittima rientri nell'ambito di applicazione del regolamento (UE) 2017/2226, del regolamento (CE) n. 767/2008 o del regolamento (UE) 2018/1240;

c) il numero delle richieste di accesso al CIR a fini di prevenzione, accertamento e indagine di reati di terrorismo o altri reati gravi;

d) il numero e i tipi di casi in cui si è giunti a un'identificazione;

e) la necessità di trattare casi eccezionali d'urgenza, compresi i casi in cui il punto di accesso centrale non ha confermato l'urgenza dopo la verifica a posteriori.

Le relazioni annuali preparate dagli Stati membri e da Europol sono trasmesse alla Commissione entro il 30 giugno dell'anno successivo.

10. Una soluzione tecnica è messa a disposizione degli Stati membri per gestire le richieste di accesso dell'utente di cui all'articolo 22 e agevolare la raccolta delle informazioni a norma dei paragrafi 7 e 9 del presente articolo ai fini dell'elaborazione delle relazioni e delle statistiche di cui a tali paragrafi. La Commissione adotta atti di esecuzione per stabilire le specifiche della soluzione tecnica. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 79

Entrata in vigore e applicazione

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

Le disposizioni del presente regolamento relative all'ESP si applicano a decorrere dalla data stabilita dalla Commissione in conformità dell'articolo 72, paragrafo 1.

Le disposizioni del presente regolamento relative al BMS comune si applicano a decorrere dalla data stabilita dalla Commissione in conformità dell'articolo 72, paragrafo 2.

Le disposizioni del presente regolamento relative al CIR si applicano a decorrere dalla data stabilita dalla Commissione in conformità dell'articolo 72, paragrafo 3.

Le disposizioni del presente regolamento relative al MID si applicano a decorrere dalla data stabilita dalla Commissione in conformità dell'articolo 72, paragrafo 4.

Le disposizioni del presente regolamento relative ai meccanismi e alle procedure di controllo della qualità dei dati automatizzati, agli indicatori comuni di qualità dei dati e alle norme minime di qualità dei dati si applicano a decorrere rispettivamente dalle date stabilite dalla Commissione in conformità dell'articolo 72, paragrafo 5.

Le disposizioni del presente regolamento relative al CRRS si applicano a decorrere dalla data stabilita dalla Commissione in conformità dell'articolo 72, paragrafo 6.

Gli articoli 6, 12, 17, 25, 38, 42, 52, 54, 56, 57, 70, 71, 73, 74, 75, 77 e 78, paragrafo 1, si applicano a decorrere dall'11 giugno 2019.

Il presente regolamento si applica in relazione all'Eurodac a decorrere dalla data in cui la rifusione del regolamento (UE) n. 603/2013 diventa applicabile.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri conformemente ai trattati.

Fatto a Bruxelles, il 20 maggio 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

REGOLAMENTO (UE) 2019/818 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 20 maggio 2019

che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, paragrafo 2, l'articolo 74, l'articolo 78, paragrafo 2, lettera e), l'articolo 79, paragrafo 2, lettera c), l'articolo 82, paragrafo 1, lettera d), l'articolo 85, paragrafo 1, l'articolo 87, paragrafo 2, lettera a), e l'articolo 88, paragrafo 2,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) Nella comunicazione del 6 aprile 2016 dal titolo «Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza», la Commissione ha sottolineato la necessità di migliorare l'architettura di gestione dei dati dell'Unione per la gestione delle frontiere e la sicurezza. La comunicazione ha dato il via a un processo mirante alla realizzazione dell'interoperabilità tra i sistemi di informazione dell'UE relativi alla sicurezza, alle frontiere e alla gestione della migrazione, allo scopo di colmare le carenze strutturali di tali sistemi che ostacolano il lavoro delle autorità nazionali, garantendo nel contempo che le guardie di frontiera, le autorità doganali, gli operatori di polizia e le autorità giudiziarie dispongano delle informazioni necessarie.

(2) Nella tabella di marcia per rafforzare lo scambio e la gestione di informazioni, comprese soluzioni di interoperabilità nel settore «Giustizia e affari interni» del 6 giugno 2016, il Consiglio ha individuato una serie di sfide giuridiche, tecniche e operative riguardanti l'interoperabilità dei sistemi di informazione dell'UE e ha sollecitato la ricerca di soluzioni.

(3) Nella risoluzione del 6 luglio 2016 sulle priorità strategiche per il programma di lavoro della Commissione per il 2017 ([3]), il Parlamento europeo ha chiesto proposte intese a migliorare e sviluppare i sistemi di informazione dell'UE esistenti, far fronte alla carenza di informazioni e progredire verso la loro interoperabilità, nonché proposte concernenti lo scambio obbligatorio di informazioni a livello dell'UE, assicurando nel contempo le necessarie garanzie in materia di protezione dei dati.

(4) Nelle conclusioni del 15 dicembre 2016 il Consiglio europeo ha sollecitato il conseguimento di ulteriori risultati sull'interoperabilità di sistemi di informazione e di banche dati dell'UE.

(5) Nella relazione finale dell'11 maggio 2017 il gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità ha concluso che era necessario e tecnicamente fattibile adoperarsi per giungere a soluzioni pratiche in materia di interoperabilità e che l'interoperabilità, in linea di massima, poteva offrire vantaggi operativi ed essere introdotta nel rispetto dei requisiti in materia di protezione dei dati.

(6) Nella comunicazione del 16 maggio 2017 contenente la «Settima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza», la Commissione, in linea con quanto esposto nella comunicazione del 6 aprile 2016 e i risultati e le raccomandazioni del gruppo ad alto livello sui sistemi di informazione e l'interoperabilità, ha delineato un nuovo approccio alla gestione dei dati relativi alle frontiere, alla sicurezza e alla migrazione, in base al quale tutti i sistemi di informazione dell'UE per la gestione della sicurezza, delle frontiere e della migrazione dovevano essere interoperabili, in maniera tale da rispettare pienamente i diritti fondamentali.

([1]) GU C 283 del 10.8.2018, pag. 48.
([2]) Posizione del Parlamento europeo del 16 aprile 2019 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 14 maggio 2019.
([3]) GU C 101 del 16.3.2018, pag. 116.

(7) Nelle conclusioni del 9 giugno 2017 sulla via da seguire per migliorare lo scambio di informazioni e garantire l'interoperabilità dei sistemi d'informazione dell'UE, il Consiglio ha invitato la Commissione a portare avanti le soluzioni di interoperabilità proposte dal gruppo di esperti ad alto livello.

(8) Nelle conclusioni del 23 giugno 2017 il Consiglio europeo ha sottolineato la necessità di migliorare l'interoperabilità fra le banche dati e ha invitato la Commissione a elaborare quanto prima un progetto di normativa sulla base delle proposte formulate dal gruppo di esperti di alto livello sui sistemi di informazione e l'interoperabilità.

(9) Per migliorare l'efficacia e l'efficienza dei controlli alle frontiere esterne, contribuire a prevenire e contrastare l'immigrazione illegale e concorrere a garantire un alto livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, incluso il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri, migliorare l'attuazione della politica comune in materia di visti, aiutare nell'esame delle domande di protezione internazionale, contribuire alla prevenzione, all'individuazione e all'indagine dei reati di terrorismo e di altri reati penali gravi, agevolare l'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati nel caso di una catastrofe naturale, incidente o attentato terroristico, al fine di preservare la fiducia dell'opinione pubblica nel sistema di migrazione e di asilo dell'Unione, nelle misure di sicurezza dell'Unione e nelle capacità dell'Unione di gestire le frontiere esterne, è opportuno rendere interoperabili i sistemi di informazione dell'Unione, vale a dire il sistema di ingressi/uscite (EES), il sistema di informazione visti (VIS), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), l'Eurodac, il sistema d'informazione Schengen (SIS) e il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (ECRIS-TCN), affinché essi si integrino reciprocamente unitamente ai relativi dati, rispettando nel contempo i diritti fondamentali degli individui, in particolare il diritto alla protezione dei dati personali. A tal fine è opportuno istituire un portale di ricerca europeo (ESP), un servizio comune di confronto biometrico (BMS comune), un archivio comune di dati di identità (CIR) e un rilevatore di identità multiple (MID) che fungano da componenti dell'interoperabilità.

(10) L'interoperabilità dovrebbe consentire a tali sistemi di informazione dell'UE di integrarsi reciprocamente al fine di facilitare la corretta identificazione delle persone, tra cui le persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati, contribuire a contrastare la frode di identità, migliorare e uniformare i requisiti in materia di qualità dei dati dei rispettivi sistemi di informazione dell'UE, agevolare l'attuazione tecnica e operativa dei sistemi di informazione dell'UE da parte degli Stati membri, rafforzare la sicurezza e protezione dei dati che presiedono ai rispettivi sistemi di informazione dell'UE, razionalizzare l'accesso, a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, all'EES, al VIS, all'ETIAS e all'Eurodac a fini di contrasto e sostenere le finalità dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e di ECRIS-TCN.

(11) Le componenti dell'interoperabilità dovrebbero includere l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS e ECRIS-TCN. Dovrebbero includere anche i dati Europol, ma soltanto in modo tale da rendere possibile la consultazione dei dati Europol simultaneamente a quella dei suddetti sistemi di informazione dell'UE.

(12) Le componenti dell'interoperabilità dovrebbero trattare i dati personali delle persone i cui dati personali sono trattati nei sistemi di informazione dell'UE sottostanti e da Europol.

(13) È opportuno istituire l'ESP al fine di facilitare, dal punto di vista tecnico, l'accesso delle autorità degli Stati membri e delle agenzie dell'Unione, in modo rapido, continuato, efficace, sistematico e controllato, ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati dell'Organizzazione internazionale della polizia criminale (Interpol), nella misura in cui ciò è necessario per svolgere i loro compiti, conformemente ai rispettivi diritti di accesso. Inoltre è opportuno istituire l'ESP al fine di sostenere gli obiettivi dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS, di ECRIS-TCN e dei dati Europol. Permettendo l'interrogazione parallela di tutti i sistemi di informazione dell'UE pertinenti, dei dati Europol e delle banche dati Interpol, l'ESP dovrebbe fungere da interfaccia unica o da mediatore di messaggi («*message broker*») per la consultazione di diversi sistemi centrali e per il recupero agevole delle informazioni necessarie, nel pieno rispetto dei requisiti concernenti il controllo degli accessi e la protezione dei dati dei sistemi sottostanti.

(14) L'ESP dovrebbe essere progettato in modo da garantire che quando interroga le banche dati Interpol i dati utilizzati da un utente ESP per avviare un'interrogazione non siano condivisi con i proprietari dei dati Interpol. L'ESP dovrebbe inoltre essere progettato in modo da garantire che le banche dati Interpol siano interrogate esclusivamente in conformità del diritto nazionale e dell'Unione applicabile.

(15) Gli utenti ESP che hanno il diritto di accedere ai dati Europol a norma del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ([4]) dovrebbero poter consultare i dati Europol simultaneamente ai sistemi di informazione dell'UE ai quali hanno accesso. Qualsiasi ulteriore trattamento dei dati successivo a tale consultazione dovrebbe avvenire a norma del regolamento (UE) 2016/794, comprese le limitazioni all'accesso o all'uso imposte dal fornitore dei dati.

(16) L'ESP dovrebbe essere sviluppato e configurato in modo tale da consentire che tali interrogazioni siano effettuate soltanto attraverso l'uso di dati riguardanti persone o documenti di viaggio presenti in un sistema di informazione dell'UE, nei dati Europol o nelle banche dati Interpol.

(17) Per garantire l'utilizzo sistematico dei pertinenti sistemi di informazione dell'UE, l'ESP dovrebbe essere usato per interrogare il CIR, l'EES, il VIS, l'ETIAS, l'Eurodac e l'ECRIS-TCN. Un collegamento nazionale ai diversi sistemi di informazione dell'UE dovrebbe tuttavia essere mantenuto, così da offrire la possibilità di ricorrere tecnicamente a una procedura sostitutiva. L'ESP dovrebbe inoltre essere utilizzato dalle agenzie dell'Unione per interrogare il SIS centrale conformemente ai rispettivi diritti di accesso e ai fini dell'espletamento dei loro compiti. Esso dovrebbe essere un mezzo supplementare per interrogare il SIS centrale, i dati Europol e le banche dati Interpol, integrando le interfacce dedicate esistenti.

(18) I dati biometrici quali le impronte digitali e le immagini del volto sono unici e di conseguenza molto più attendibili dei dati alfanumerici ai fini dell'identificazione di una persona. Il BMS comune dovrebbe essere uno strumento tecnico da utilizzare per rafforzare e agevolare il lavoro dei sistemi di informazione dell'UE pertinenti e delle altre componenti dell'interoperabilità. Lo scopo principale del BMS comune dovrebbe essere l'agevolazione dell'identificazione di una persona che è registrata in diverse banche dati utilizzando un'unica componente tecnologica per far corrispondere i dati biometrici di quella persona contenuti in diversi sistemi anziché più componenti. Il BMS comune dovrebbe contribuire alla sicurezza e offrire vantaggi in termini finanziari, operativi e di manutenzione. Tutti i sistemi automatizzati di identificazione dattiloscopica, inclusi quelli attualmente utilizzati per l'Eurodac, il VIS e il SIS, usano template biometrici costituiti da dati ricavati mediante estrazione di parametri di campioni biometrici effettivi. Il BMS comune dovrebbe riunire e conservare tutti i template biometrici – separati per logica in base al sistema di informazione di provenienza – in un unico luogo, facilitando il confronto trasversale ai vari sistemi mediante l'uso di template biometrici e permettendo economie di scala nello sviluppo e nella manutenzione dei sistemi centrali dell'UE.

(19) I template biometrici conservati nel BMS comune dovrebbero essere costituiti da dati ricavati mediante estrazione di parametri di campioni biometrici effettivi e ottenuti in modo tale che non sia possibile invertire il processo di estrazione. I template biometrici dovrebbero essere ottenuti da dati biometrici, ma non dovrebbe essere possibile ottenere gli stessi dati biometrici dai template biometrici. Poiché i dati sulle impronte palmari e i profili DNA sono conservati unicamente nel SIS e non possono essere utilizzati a fini di controlli incrociati con i dati contenuti in altri sistemi di informazione, seguendo i principi di necessità e proporzionalità, il BMS comune non dovrebbe conservare i profili DNA o i template biometrici ottenuti dai dati sulle impronte palmari.

(20) I dati biometrici sono dati personali sensibili. Il presente regolamento dovrebbe stabilire le basi e le garanzie per il trattamento di tali dati allo scopo di identificare in modo univoco le persone interessate.

(21) I sistemi EES, VIS, ETIAS, Eurodac e ECRIS-TCN richiedono l'identificazione precisa delle persone di cui conservano i dati personali. Il CIR dovrebbe pertanto agevolare la corretta identificazione delle persone registrate in tali sistemi.

(22) I dati personali conservati nei sistemi di informazione dell'UE possono riferirsi alle stesse persone, ma con identità differenti o incomplete. Gli Stati membri dispongono di modalità efficaci per identificare i propri cittadini o residenti permanenti iscritti nel loro territorio. L'interoperabilità tra i sistemi di informazione dell'UE dovrebbe contribuire alla corretta identificazione delle persone presenti in tali sistemi. CIR dovrebbe conservare i dati personali necessari per consentire un'identificazione più precisa delle persone i cui dati sono conservati in tali sistemi, compresi i dati di identità, i dati del documento di viaggio e i dati biometrici, a prescindere dal sistema nel quale tali dati sono stati inizialmente raccolti. Il CIR dovrebbe conservare solo i dati personali strettamente necessari per svolgere una verifica di identità accurata. I dati personali che vi sono registrati dovrebbero essere conservati per un arco di tempo non superiore a quanto strettamente necessario per il conseguimento delle finalità dei sistemi sottostanti e sono cancellati in modo automatico e concomitante alla loro cancellazione dai sistemi sottostanti, in base alla separazione logica.

([4]) 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).

(23) Una nuova operazione di trattamento consistente nel conservare questo tipo di dati nel CIR anziché in ciascun sistema separato è necessaria al fine di migliorare l'accuratezza dell'identificazione attraverso il confronto e l'abbinamento automatizzati dei dati. Il fatto che i dati di identità, i dati del documento di viaggio e biometrici siano conservati nel CIR non dovrebbe ostacolare in alcun modo il trattamento dei dati ai fini di EES, VIS, ETIAS, Eurodac o ECRIS-TCN, poiché il CIR dovrebbe essere una nuova componente comune di tali sistemi sottostanti.

(24) È necessario pertanto creare un fascicolo individuale nel CIR per ogni persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o in ECRIS-TCN ai fini di una corretta identificazione dei cittadini di paesi terzi all'interno dello spazio Schengen e quale supporto al funzionamento del MID, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. Il fascicolo individuale dovrebbe conservare tutte le informazioni relative all'identità connesse a una data persona in un unico luogo e renderle accessibili agli utenti finali debitamente autorizzati.

(25) Il CIR dovrebbe pertanto agevolare e semplificare l'accesso delle autorità responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o altri reati gravi ai sistemi di informazione dell'UE che non sono istituiti esclusivamente a fini di prevenzione, accertamento o indagine di reati gravi.

(26) Il CIR dovrebbe offrire un contenitore comune per i dati di identità, i dati del documento di viaggio e biometrici delle persone registrate nell'EES, nel VIS, nell'ETIAS, nell'Eurodac e nell'ECRIS-TCN. Dovrebbe rientrare nell'architettura tecnica di tali sistemi e fungere da componente comune tra di essi ai fini della conservazione e dell'interrogazione dei dati di identità, dei dati del documento di viaggio e biometrici che trattano.

(27) Tutte le registrazioni nel CIR dovrebbero essere separate logicamente mediante l'apposizione automatica, su ciascuna di esse, di un'etichetta che indichi il nome del sistema sottostante da cui provengono. Il sistema di controllo degli accessi del CIR dovrebbe utilizzare queste etichette per determinare se consentire o meno l'accesso alle registrazioni.

(28) Ove un'autorità di polizia di uno Stato membro non sia in grado di identificare una persona in ragione dell'assenza di un documento di viaggio o di un altro documento credibile che ne dimostri l'identità, ovvero ove sussistano dubbi quanto ai dati di identità forniti dall'interessato o all'autenticità del documento di viaggio o all'identità del titolare, ovvero qualora l'interessato non sia in grado o rifiuti di cooperare, l'autorità in questione dovrebbe essere in grado di interrogare il CIR al fine di identificare la persona in oggetto. A tal fine, le autorità di polizia dovrebbero rilevare le impronte digitali utilizzando tecniche di scansione diretta (*live-scan*), a condizione che la procedura sia avviata in presenza di tale persona. Tali interrogazioni del CIR non dovrebbero essere autorizzate ai fini dell'identificazione di minori di età inferiore a 12 anni, a meno che ciò non sia nell'interesse superiore del minore.

(29) Se non si possono usare i dati biometrici dell'interessato o se un'interrogazione con tali dati non dà alcun esito, l'interrogazione dovrebbe essere effettuata con i dati di identità dell'interessato combinati con i dati del documento di viaggio. Se dall'interrogazione emerge che dati relativi all'interessato sono conservati nel CIR, le autorità dello Stato membro dovrebbero avere accesso al CIR per la consultazione dei dati di identità e dei dati del documento di viaggio di tale persona, senza che il CIR fornisca alcuna indicazione sul sistema di informazione dell'UE cui appartengono tali dati.

(30) Gli Stati membri dovrebbero adottare misure legislative nazionali per designare le autorità competenti a svolgere le verifiche di identità utilizzando il CIR e stabilendo le procedure, le condizioni e i criteri di queste verifiche, le quali dovrebbero rispettare principio di proporzionalità. Dette misure, in particolare, dovrebbero conferire a tali autorità il potere di raccogliere dati biometrici della persona durante una verifica di identità effettuata in presenza di un loro rappresentante.

(31) Il presente regolamento dovrebbe altresì introdurre per le autorità designate dallo Stato membro responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o altri reati gravi e per Europol una nuova possibilità di accesso semplificato ad altri dati rispetto a quelli di identità o a quelli del documento di viaggio presenti nell'EES, nel VIS, nell'ETIAS o nell'Eurodac. Tali dati possono essere necessari, in casi specifici, a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, ove vi siano motivi ragionevoli per ritenere che la loro consultazione contribuirà alla prevenzione, all'accertamento o all'indagine dei reati di terrorismo o degli altri reati gravi, in particolare qualora sussista il sospetto che la persona sospettata, l'autore o la vittima di un reato di terrorismo o di un altro reato grave è una persona i cui dati sono conservati nell'EES, nel VIS, nell'ETIAS o nell'Eurodac.

(32) Il pieno accesso ai dati contenuti nell'EES, nel VIS, nell'ETIAS o nell'Eurodac che sia necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, diverso dall'accesso ai dati di identità o ai dati del documento di viaggio contenuti nel CIR, dovrebbe continuare a essere disciplinato dagli strumenti giuridici applicabili. Le autorità designate responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o altri reati gravi ed Europol non sanno in anticipo quale sistema di informazione dell'UE contenga dati sulle persone su cui devono compiere indagini. Ciò causa ritardi e inefficienze. Di conseguenza, l'utente finale autorizzato dall'autorità designata dovrebbe avere la facoltà di vedere in quale di tali sistemi di informazione dell'UE sono registrati i dati corrispondenti al risultato dell'interrogazione. Il sistema interessato verrebbe pertanto segnalato in esito alla verifica automatica della presenza di un riscontro positivo nel sistema (la cosiddetta funzione di segnalazione «*match/no match*»).

(33) In tale contesto, la risposta dal CIR non dovrebbe essere interpretata o utilizzata come motivo o ragione per trarre conclusioni o adottare misure riguardo a una persona, ma dovrebbe essere utilizzata soltanto per presentare una richiesta di accesso ai sistemi di informazione sottostanti dell'UE soggetta alle condizioni e alle procedure stabilite dai rispettivi strumenti giuridici che regolamentano tale accesso. Qualsiasi richiesta di accesso di questo genere dovrebbe essere soggetta al capo VII del presente regolamento e, laddove applicabile, al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([5]), alla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([6]) o al regolamento (UE) 2016/1725 del Parlamento europeo e del Consiglio ([7]).

(34) In linea di massima, se da un riscontro positivo emerge che i dati sono registrati nell'Eurodac, è opportuno che le autorità designate o Europol richiedano il pieno accesso ad almeno uno dei sistemi di informazione dell'UE interessati. Ove, in via eccezionale, tale accesso integrale non sia richiesto, per esempio perché le autorità designate o Europol hanno già ottenuto i dati con altri mezzi o se il diritto nazionale non consente più di ottenere tali dati, è auspicabile registrare la motivazione della mancata richiesta di accesso.

(35) Le registrazioni delle interrogazioni nel CIR dovrebbero indicare lo scopo delle interrogazioni Se l'interrogazione è stata effettuata utilizzando l'approccio di consultazione dei dati in due fasi, le registrazioni dovrebbero contenere un riferimento al fascicolo nazionale dell'indagine o del caso, indicando perciò che essa è stata avviata a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi.

(36) L'interrogazione del CIR da parte delle autorità designate e di Europol al fine di ottenere un riscontro che segnali la presenza o meno di dati nell'EES, nel VIS, nell'ETIAS o nell'Eurodac, richiede il trattamento automatizzato dei dati personali. La segnalazione del riscontro positivo non dovrebbe rivelare i dati personali dell'interessato, ma si limiterebbe a indicare che alcuni dei suoi dati sono conservati in uno dei sistemi. L'utente finale autorizzato non dovrebbe assumere alcuna decisione sfavorevole all'interessato basandosi unicamente sulla semplice segnalazione di un riscontro positivo. L'accesso dell'utente finale a tale segnalazione costituirà pertanto un'ingerenza molto limitata nel diritto alla protezione dei dati personali dell'interessato, consentendo allo stesso tempo alle autorità designate e a Europol di richiedere l'accesso ai dati personali in modo più efficace.

(37) È opportuno istituire il MID per sostenere il funzionamento del CIR, nonché gli obiettivi dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e di ECRIS-TCN. Per poter realizzare efficacemente i loro rispettivi obiettivi, questi sistemi di informazione dell'UE richiedono tutti un'identificazione precisa delle persone di cui conservano i dati personali.

(38) Ai fini di un migliore conseguimento degli obiettivi dei sistemi di informazione dell'UE, le autorità che li utilizzano dovrebbero poter effettuare verifiche sufficientemente affidabili dell'identità delle persone i cui dati sono conservati in sistemi diversi. L'insieme di dati di identità o di dati del documento di viaggio può essere

([5]) 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).

([6]) 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).

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

inesatto, incompleto o fraudolento e, a oggi, non vi è alcun modo per rilevare dati di identità o dati del documento di viaggio fraudolenti, inesatti o incompleti mediante un confronto con i dati conservati in un altro sistema. Per rimediare a questa situazione è necessario dotarsi, a livello dell'Unione, di uno strumento tecnico che consenta un'identificazione precisa delle persone per tali scopi.

(39) Il MID dovrebbe creare e conservare i collegamenti tra i dati presenti nei vari sistemi di informazione dell'UE ai fini dell'individuazione di identità multiple, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. Il MID dovrebbe contenere solo i collegamenti tra i dati sulle persone fisiche presenti in più di un sistema di informazione dell'UE. I dati collegati dovrebbero essere rigorosamente limitati ai dati necessari per verificare se l'interessato è registrato in maniera giustificata o ingiustificata e con identità diverse in sistemi diversi, ovvero per chiarire che due persone aventi dati di identità simili possono non essere la stessa persona. Il trattamento dei dati mediante l'ESP e il BMS comune al fine di collegare i fascicoli individuali trasversalmente ai diversi sistemi dovrebbe limitarsi al minimo indispensabile e, pertanto, alla semplice rilevazione di un'identità multipla da condurre nel momento in cui sono aggiunti nuovi dati a uno dei sistemi che ha i dati raccolti nel CIR e nel SIS. Il MID dovrebbe prevedere misure di salvaguardia che tutelino le persone con identità multiple lecite da eventuali discriminazioni e decisioni sfavorevoli.

(40) Il presente regolamento prevede nuove operazioni di trattamento dei dati miranti a identificare in modo corretto le persone interessate. Ciò costituisce un'ingerenza nei loro diritti fondamentali tutelati dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Poiché l'attuazione efficace dei sistemi di informazione dell'UE dipende dalla corretta identificazione delle persone interessate, tale ingerenza è giustificata dagli stessi obiettivi per i quali ciascuno di questi sistemi è stato istituito, vale a dire: la gestione efficace delle frontiere dell'Unione, la sicurezza interna dell'Unione e l'attuazione efficace delle politiche dell'Unione in materia di asilo e di visti.

(41) Quando un'autorità nazionale o un'agenzia dell'Unione crea o carica nuove registrazioni, l'ESP e il BMS comune dovrebbero confrontare i dati riguardanti le persone contenuti nel CIR e nel SIS. Tale confronto dovrebbe essere automatizzato. Il CIR e il SIS dovrebbero utilizzare il BMS comune per individuare eventuali collegamenti sulla base dei dati biometrici. Dovrebbero utilizzare l'ESP per individuare eventuali collegamenti sulla base dei dati alfanumerici. Il CIR e il SIS dovrebbero essere in grado di individuare i dati identici o simili concernenti una persona conservati in più sistemi. In tal caso dovrebbe essere creato un collegamento che indichi che si tratta della stessa persona. Il CIR e il SIS dovrebbero essere configurati in modo tale da individuare i piccoli errori di ortografia o di traslitterazione, così da non creare ostacoli ingiustificati all'interessato.

(42) L'autorità nazionale o l'agenzia dell'Unione che ha registrato i dati nel sistema di informazione dell'UE pertinente dovrebbe confermare o modificare tali collegamenti. Tale autorità nazionale o l'agenzia dell'Unione dovrebbe avere accesso ai dati conservati nel CIR o nel SIS e nel MID ai fini della verifica manuale di diverse identità.

(43) Una verifica manuale delle diverse identità dovrebbe competere all'autorità che ha creato o aggiornato i dati per i quali è emerso un riscontro positivo, che a sua volta ha dato luogo a un collegamento con i dati conservati in un altro sistema di informazione dell'UE. L'autorità responsabile della verifica manuale delle diverse identità dovrebbe accertare se esistano più identità che si riferiscono alla stessa persona in maniera giustificata o ingiustificata. Tale accertamento deve aver luogo, se possibile, in presenza della persona interessata, se del caso chiedendo ulteriori chiarimenti o informazioni. Dovrebbe essere effettuato senza indugio, nel rispetto dei requisiti giuridici riguardanti l'accuratezza delle informazioni ai sensi del diritto nazionale e dell'Unione.

(44) Per i collegamenti ottenuti attraverso il SIS relativamente a segnalazioni di persone ricercate per l'arresto a fini di consegna o di estradizione, di persone scomparse o vulnerabili, di persone ricercate per presenziare a un procedimento giudiziario o di persone da sottoporre a controllo discreto o a controllo di indagine, l'autorità responsabile della verifica manuale delle diverse identità dovrebbe essere l'ufficio SIRENE dello Stato membro che

ha creato la segnalazione. Tali categorie di segnalazioni SIS sono sensibili e non dovrebbero essere necessariamente condivise con le autorità che inseriscono o aggiornano i dati collegati a essi in uno degli altri sistemi di informazione dell'UE. La creazione di un collegamento con i dati del SIS dovrebbe lasciare impregiudicate le azioni da intraprendere a norma dei regolamenti (UE) 2018/1860 ([8]), (UE) 2018/1861 ([9]) e (UE) 2018/1862 ([10]) del Parlamento europeo e del Consiglio.

(45) La creazione di tali collegamenti esige un atteggiamento trasparente nei confronti degli interessati. Al fine di agevolare l'attuazione delle necessarie garanzie in conformità delle norme applicabili dell'Unione in materia di protezione dei dati, le persone fisiche che, a seguito di una verifica manuale delle identità diverse, sono oggetto di un collegamento rosso o un collegamento bianco dovrebbero esserne informate per iscritto, fatte salve le limitazioni necessarie per proteggere la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non siano compromesse indagini nazionali. Tali persone fisiche dovrebbero ricevere un numero di identificazione unico che consenta loro di identificare l'autorità cui dovrebbero rivolgersi per esercitare i propri diritti.

(46) Qualora sia creato un collegamento giallo l'autorità responsabile della verifica manuale delle identità diverse dovrebbe avere accesso al MID. Qualora esista un collegamento rosso, le autorità degli Stati membri e le agenzie dell'Unione che hanno accesso ad almeno un sistema di informazione incluso nel CIR o al SIS dovrebbero avere accesso al MID. Il collegamento rosso dovrebbe indicare che una persona utilizza identità diverse in modo ingiustificato o che una persona utilizza l'identità di un'altra.

(47) Qualora esista un collegamento bianco o verde tra dati di due sistemi di informazione dell'UE, le autorità degli Stati membri e delle agenzie dell'Unione dovrebbero avere accesso al MID se l'autorità o agenzia interessata abbia accesso a entrambi i sistemi di informazione. Tale accesso dovrebbe essere accordato al solo scopo di consentire a tale autorità o agenzia di individuare potenziali casi di collegamento inesatto o in cui il trattamento dei dati nel MID, nel CIR e nel SIS è avvenuto in violazione del presente regolamento, e di adottare l'azione per correggere la situazione e aggiornare o cancellare il collegamento.

(48) L'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) dovrebbe istituire meccanismi automatizzati di controllo della qualità dei dati e indicatori comuni della qualità dei dati. eu-LISA dovrebbe essere responsabile dello sviluppo di una capacità centrale di monitoraggio della qualità dei dati e della redazione di relazioni periodiche di analisi dei dati, allo scopo di migliorare il controllo dell'attuazione dei sistemi di informazione dell'UE da parte degli Stati membri. Gli indicatori comuni sui dati dovrebbero includere norme minime di qualità per la conservazione dei dati nei sistemi di informazione dell'UE o nelle componenti dell'interoperabilità. Tali norme di qualità dei dati dovrebbero avere come obiettivo quello di consentire ai sistemi di informazione dell'UE e alle componenti dell'interoperabilità di individuare automaticamente i dati inviati che sono palesemente errati o incoerenti, affinché lo Stato membro da cui provengono sia in grado di verificarli e di provvedere a tutte le misure correttive necessarie.

(49) La Commissione dovrebbe valutare le relazioni di eu-LISA riguardanti la qualità e, se del caso, dovrebbe rivolgere raccomandazioni agli Stati membri. Gli Stati membri dovrebbero elaborare un piano d'azione che illustri le misure correttive volte a colmare le eventuali carenze nella qualità dei dati e dovrebbero riferire regolarmente in merito ai progressi compiuti.

(50) Il formato universale dei messaggi (UMF) dovrebbe fungere quale standard per lo scambio strutturato delle informazioni a livello transfrontaliero tra i sistemi di informazione, le autorità o le organizzazioni del settore Giustizia e affari interni. Per le informazioni scambiate abitualmente, l'UMF dovrebbe definire un lessico comune e strutture logiche che facilitino l'interoperabilità permettendo la creazione e la lettura del contenuto dello scambio in modo coerente e semanticamente equivalente.

(51) L'attuazione dello standard UMF può essere contemplata per il VIS, il SIS e qualunque altro modello esistente per lo scambio di informazioni o sistema di informazione transfrontaliero, nuovo o esistente, del settore Giustizia e affari interni sviluppato dagli Stati membri.

([8]) Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 312 del 7.12.2018, pag. 1).

([9]) Regolamento (UE) 2018/1861 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 (GU L 312 del 7.12.2018, pag. 14).

([10]) Regolamento (UE) 2018/1862 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 della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).

(52) È opportuno istituire un archivio centrale di relazioni e statistiche (CRRS) al fine di generare dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati, in conformità degli strumenti giuridici applicabili. eu-LISA dovrebbe istituire, attuare e ospitare il CRRS nei suoi siti tecnici. Dovrebbe contenere dati statistici anonimi provenienti dai sistemi di informazione dell'UE, dal CIR, dal MID e dal BMS comune. I dati contenuti nel CRRS non dovrebbero permettere l'identificazione delle persone fisiche. eu-LISA dovrebbe anonimizzare automaticamente i dati e dovrebbe registrare nel CRRS i dati così anonimizzati. Il processo di anonimizzazione dovrebbe essere automatizzato e il personale di eu-LISA non dovrebbe essere autorizzato in alcun modo ad accedere direttamente ai dati personali conservati nei sistemi di informazione dell'UE o nelle componenti dell'interoperabilità.

(53) Il regolamento (UE) 2016/679 si applica al trattamento dei dati personali ai fini dell'interoperabilità nell'ambito del presente regolamento da parte delle autorità nazionali, a meno che tale trattamento non sia effettuato dalle autorità designate o dai punti di accesso centrale degli Stati membri a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi.

(54) Qualora il trattamento di dati personali da parte degli Stati membri finalizzato all'interoperabilità ai sensi del presente regolamento sia effettuato dalle autorità competenti a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, si applica la direttiva (UE) 2016/680.

(55) Il regolamento (UE) 2016/679, il regolamento (UE) 2018/1725 o, se del caso, la direttiva (UE) 2016/680 si applicano a qualsiasi trasferimento di dati personali verso paesi terzi o organizzazioni internazionali effettuati ai sensi del presente regolamento. Fatti salvi i motivi di trasferimento a norma del capo V del regolamento (UE) 2016/679 o, se del caso, della direttiva (UE) 2016/680, le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento dovrebbero essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro.

(56) Le disposizioni specifiche sulla protezione dei dati di cui al regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio e al regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio ([11]) si applicano al trattamento dei dati personali nei sistemi disciplinati da detti regolamenti.

(57) Il regolamento (UE) 2018/1725 si applica al trattamento dei dati personali da parte di eu-LISA e di altre istituzioni e organi dell'Unione nell'assolvimento delle loro responsabilità a norma del presente regolamento, fatto salvo il regolamento (UE) 2016/794, che si applica al trattamento dei dati personali da parte di Europol.

(58) Le autorità di controllo di cui al regolamento (UE) 2016/679 o alla direttiva (UE) 2016/680 dovrebbero verificare la legittimità del trattamento dei dati personali da parte degli Stati membri. Il garante europeo della protezione dei dati dovrebbe sorvegliare le attività delle istituzioni e degli organismi dell'Unione connesse al trattamento dei dati personali. Il garante europeo della protezione dei dati e le autorità di controllo dovrebbero collaborare nel sorvegliare il trattamento dei dati personali da parte delle componenti dell'interoperabilità. Affinché il garante europeo della protezione dei dati assolva i compiti che gli sono affidati dal presente regolamento, sono necessarie risorse sufficienti, in particolare risorse umane e finanziarie.

(59) 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 ([12]) e ha espresso un parere il 16 aprile 2018 ([13]).

(60) Il gruppo di lavoro «Articolo 29» sulla protezione dei dati ha fornito un parere l'11 aprile 2018.

(61) Sia gli Stati membri che eu-LISA dovrebbero dotarsi di piani di sicurezza che agevolino l'adempimento degli obblighi in tal senso e dovrebbero collaborare per poter risolvere le questioni relative alla sicurezza. eu-LISA dovrebbe inoltre assicurare l'uso continuo dei più recenti sviluppi tecnologici, al fine di garantire l'integrità dei dati nel contesto dello sviluppo, della progettazione e della gestione delle componenti dell'interoperabilità. Gli

([11]) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per l'identificazione degli Stati membri che forniscono informazioni sulle condanne dei cittadini di paesi terzi e degli apolidi (ECRIS-TCN), a integrazione del sistema europeo di informazione sui casellari giudiziari e che modifica il regolamento (UE) 2018/1726 (Cfr. pag. 1 della presente Gazzetta ufficiale).

([12]) 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).

([13]) GU C 233 del 4.7.2018, pag. 12.

obblighi di eu-LISA a tal riguardo dovrebbero includere l'adozione delle misure necessarie per impedire l'accesso delle persone non autorizzate, per esempio il personale dei fornitori esterni di servizi, ai dati personali trattati attraverso le componenti dell'interoperabilità. In sede di aggiudicazione dei contratti per la prestazione di servizi, gli Stati membri ed eu-LISA dovrebbero considerare tutte le misure necessarie per garantire la conformità alle disposizioni legislative e regolamentari in materia di protezione dei dati personali e della vita privata delle persone fisiche o per salvaguardare interessi essenziali di sicurezza, conformemente al regolamento (UE) 2018/1046 del Parlamento europeo e del Consiglio ([14]) e alle convenzioni internazionali applicabili. eu-LISA dovrebbe applicare i principi della tutela della vita privata fin dalla progettazione e per impostazione predefinita durante la fase di sviluppo delle componenti dell'interoperabilità.

(62) A sostegno dell'elaborazione di statistiche e relazioni, è necessario concedere al personale autorizzato delle autorità competenti, delle istituzioni dell'Unione e delle agenzie di cui al presente regolamento l'accesso alla consultazione di taluni dati relativi a determinate componenti dell'interoperabilità, senza permettere l'identificazione delle persone interessate.

(63) Per consentire alle autorità dello Stato membro e alle agenzie dell'Unione di adeguarsi ai nuovi requisiti relativi all'uso dell'ESP è necessario prevedere un periodo transitorio. Analogamente, dovrebbero essere stabilite misure transitorie per l'entrata in funzione del MID, al fine di consentirne un funzionamento coerente e ottimale.

(64) Poiché l'obiettivo del presente regolamento, vale a dire l'istituzione di un quadro per l'interoperabilità tra i sistemi di informazione dell'UE, non può essere conseguito in misura sufficiente dagli Stati membri ma può, a motivo della portata e degli effetti dell'azione in questione, essere conseguito 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 tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(65) L'importo rimanente della dotazione di bilancio destinata alle «frontiere intelligenti» di cui al regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio ([15]) dovrebbe essere riassegnato al presente regolamento, ai sensi dell'articolo 5, paragrafo 5, lettera b), del regolamento (UE) n. 515/2014, per coprire i costi di sviluppo delle componenti dell'interoperabilità.

(66) Al fine di integrare alcuni aspetti tecnici dettagliati del presente regolamento, è opportuno delegare alla Commissione il potere di adottare atti in conformità dell'articolo 290 del trattato sul funzionamento dell'Unione europea (TFUE) che riguardino:

— la proroga del periodo transitorio per l'uso dell'ESP;

— la proroga del periodo transitorio per l'uso del MID dall'unità centrale ETIAS;

— le procedure per stabilire i casi in cui i dati di identità possono essere considerati identici o simili;

— le norme relative al funzionamento del CRRS, comprese le garanzie specifiche per il trattamento dei dati personali e le norme di sicurezza applicabili all'archivio; e

— norme dettagliate concernenti il funzionamento del portale web.

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 ([16]). In particolare, al fine di garantire una partecipazione paritaria alla preparazione degli atti delegati, è opportuno che il Parlamento europeo e il Consiglio ricevano l'intera documentazione contemporaneamente agli esperti degli Stati membri e che i loro esperti abbiano sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti.

(67) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione per fissare le date a partire dalle quali l'ESP, il BMS comune, il CIR, il MID e il CRRS dovranno entrare in funzione.

([14]) Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012 (GU L 193 del 30.7.2018, pag. 1).

([15]) 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).

([16]) GU L 123 del 12.5.2016, pag. 1.

(68) È altresì opportuno attribuire alla Commissione competenze di esecuzione per l'adozione di norme dettagliate riguardanti: le modalità tecniche dei profili per gli utenti dell'ESP; le specifiche delle soluzioni tecniche che consentono le interrogazioni dei sistemi di informazione dell'UE, dei dati di Europol e delle banche dati Interpol attraverso l'ESP, nonché il formato delle risposte dell'ESP; le norme tecniche per la creazione di collegamenti nel MID tra dati di diversi sistemi di informazione dell'UE; il contenuto e la presentazione del modulo da utilizzare per informare l'interessato in caso di creazione di un collegamento rosso; i requisiti di prestazione e monitoraggio delle prestazioni del BMS comune; i meccanismi, procedure e indicatori automatizzati di controllo della qualità dei dati; lo sviluppo dello standard UMF; la procedura di cooperazione in caso di incidenti di sicurezza; e le specifiche della soluzione tecnica per la gestione delle richieste di accesso degli utenti da parte degli Stati membri. È opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([17]).

(69) Poiché le componenti dell'interoperabilità comporteranno il trattamento di quantità significative di dati personali sensibili, è importante che le persone i cui dati sono trattati tramite dette componenti possano esercitare effettivamente i loro diritti in quanto interessati come prescritto a norma del regolamento (UE) 2016/679, della direttiva (UE) 2016/680 e del regolamento (UE) 2018/1725. Gli interessati dovrebbero disporre di un portale web che li agevoli nell'esercizio dei diritti di accesso, rettifica, cancellazione e limitazione del trattamento dei loro dati personali. eu-LISA dovrebbe istituire e gestire tale portale web.

(70) Uno dei principi fondamentali della protezione dei dati personali è la minimizzazione dei dati: ai sensi dell'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679 il trattamento dei dati personali deve essere adeguato, pertinente e limitato al minimo necessario rispetto alle finalità perseguite. Per questo motivo, le componenti dell'interoperabilità non dovrebbero prevedere la conservazione di nuovi dati personali, a eccezione dei collegamenti che saranno conservati nel MID e che costituiscono il minimo indispensabile ai fini del presente regolamento.

(71) È opportuno che il presente regolamento preveda disposizioni chiare in materia di responsabilità e il diritto al risarcimento per danni causati dal trattamento illecito di dati personali e da qualsiasi altro atto incompatibile con esso. Tali disposizioni dovrebbero far salvi il diritto al risarcimento e la responsabilità da parte del titolare del trattamento o del responsabile del trattamento ai sensi del regolamento (UE) 2016/679, della direttiva (UE) 2016/680, e del regolamento (UE) 2018/1725. eu-LISA dovrebbe rispondere dei danni da essa causati in quanto responsabile del trattamento se non ha adempiuto gli obblighi del presente regolamento specificatamente gravanti su di essa o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni dello Stato membro titolare del trattamento.

(72) Il presente regolamento non pregiudica l'applicazione della direttiva 2004/38/CE del Parlamento europeo e del Consiglio ([18]).

(73) 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, nella misura in cui le sue disposizioni riguardano il SIS disciplinato dal regolamento (UE) n. 2018/1862, si basa sull'*acquis* di Schengen, la Danimarca decide, ai sensi dell'articolo 4 di tale protocollo, entro sei mesi dalla decisione del Consiglio sul presente regolamento, se intende recepirlo nel proprio diritto interno.

(74) Per quanto riguarda le disposizioni relative al SIS disciplinato dal regolamento (UE) 2018/1862, il Regno Unito partecipa al presente regolamento ai sensi dell'articolo 5, paragrafo 1, del protocollo n. 19 sull'*acquis* di Schengen integrato nell'ambito dell'Unione europea, allegato al TUE e al TFUE e dell'articolo 8, paragrafo 2, della decisione 2000/365/CE del Consiglio ([19]). Inoltre, nella misura in cui le sue disposizioni riguardano Eurodac e ECRIS-TCN, a norma dell'articolo 3 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, il Regno Unito ha notificato, con lettera del 18 maggio 2018, che desidera partecipare all'adozione e all'applicazione del presente regolamento.

([17]) 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).

([18]) 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).

([19]) 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).

(75) Nella misura in cui le sue disposizioni riguardano il SIS disciplinato dal regolamento (UE) 2018/1862, l'Irlanda potrebbe, in linea di principio, partecipare al presente regolamento ai sensi dell'articolo 5, paragrafo 1, del protocollo n. 19 sull'*acquis* di Schengen integrato nell'ambito dell'Unione europea, allegato al TUE e al TFUE, e dell'articolo 6, paragrafo 2, della decisione 2002/192/CE del Consiglio ([20]). Inoltre, nella misura in cui le sue disposizioni riguardano Eurodac ed ECRIS-TCN, a norma degli articoli 1 e 2 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda non partecipa all'adozione del presente regolamento, non è da esso vincolata né è soggetta alla sua applicazione. Poiché non è possibile, in tali circostanze, garantire che il presente regolamento sia interamente applicabile all'Irlanda, come richiesto dall'articolo 288 TFUE, l'Irlanda non partecipa all'adozione del presente regolamento e non è vincolata da esso o soggetta alla sua applicazione, fatti salvi i suoi diritti a norma dei protocolli n. 19 e n. 21.

(76) Per quanto riguarda l'Islanda e la Norvegia, il presente regolamento costituisce, per quanto riguarda il SIS disciplinato dal regolamento (UE) 2018/1862, uno sviluppo delle disposizioni dell'*acquis* di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sull'associazione di questi ultimi all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen ([21]), che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE del Consiglio ([22]).

(77) Per quanto riguarda la Svizzera, il presente regolamento costituisce, nella misura in cui si riferisce al SIS disciplinato dal regolamento (UE) 2018/1862, uno sviluppo delle disposizioni dell'*acquis* di Schengen ai sensi 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 ([23]) che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE, in combinato disposto con l'articolo 3 della decisione 2008/149/GAI del Consiglio ([24]).

(78) Per quanto riguarda il Liechtenstein, il presente regolamento costituisce, nella misura in cui si riferisce al SIS disciplinato dal regolamento (UE) 2018/1862, uno sviluppo delle disposizioni dell'*acquis* di Schengen 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 ([25]) che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE, in combinato disposto con l'articolo 3 della decisione 2011/350/UE del Consiglio ([26]).

(79) Il presente regolamento rispetta i diritti fondamentali e osserva i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea e dovrebbe essere applicato conformemente a tali diritti e principi.

(80) Per integrare il presente regolamento nel quadro giuridico esistente, è opportuno modificare di conseguenza il regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio ([27]) e i regolamenti (UE) 2018/1862 e (UE) 2019/816,

---

([20]) 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).

([21]) GU L 176 del 10.7.1999, pag. 36.

([22]) 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).

([23]) GU L 53 del 27.2.2008, pag. 52.

([24]) Decisione 2008/149/GAI del Consiglio, del 28 gennaio 2008, relativa alla conclusione, a nome dell'Unione 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. 50).

([25]) GU L 160 del 18.6.2011, pag. 21.

([26]) 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).

([27]) Regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, 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 295 del 21.11.2018, pag. 99).

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

Disposizioni generali

Articolo 1

Oggetto

1. Il presente regolamento, unitamente al regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio ([28]), istituisce un quadro per garantire l'interoperabilità tra il sistema di ingressi/uscite (EES), il sistema di informazione visti (VIS), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), l'Eurodac, il sistema d'informazione Schengen (SIS) e il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (ECRIS-TCN).

2. Il quadro consta delle seguenti componenti dell'interoperabilità:

a) un portale di ricerca europeo (ESP);

b) un servizio comune di confronto biometrico (BMS comune);

c) un archivio comune di dati di identità (CIR);

d) un rilevatore di identità multiple (MID).

3. Il presente regolamento fissa le disposizioni relative ai requisiti di qualità dei dati, al formato universale dei messaggi (UMF) e a un archivio centrale di relazioni e statistiche (CRRS), e sulle responsabilità degli Stati membri e dell'Agenzia europea per la gestione operativa di sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) per quanto riguarda la progettazione, lo sviluppo e il funzionamento delle componenti dell'interoperabilità.

4. Il presente regolamento adatta le procedure e le condizioni per l'accesso delle autorità designate e dell'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) all'EES, al VIS, all'ETIAS e all'Eurodac a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi.

5. Il presente regolamento stabilisce inoltre un quadro per il controllo delle identità delle persone e per l'identificazione delle persone.

Articolo 2

Obiettivi

1. Garantendo l'interoperabilità il presente regolamento persegue i seguenti obiettivi:

a) migliorare l'efficacia e l'efficienza delle verifiche di frontiera alle frontiere esterne;

b) contribuire a prevenire e combattere l'immigrazione illegale;

c) contribuire ad 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;

d) migliorare l'attuazione della politica comune in materia di visti;

e) aiutare nell'esame delle domande di protezione internazionale;

f) contribuire alla prevenzione, all'accertamento e all'indagine di reati di terrorismo o altri reati gravi;

g) facilitare l'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati nel caso di una catastrofe naturale, incidente o attentato terroristico.

2. Gli obiettivi di cui al paragrafo 1 sono realizzati:

a) garantendo la corretta identificazione delle persone;

b) contribuendo a combattere la frode di identità;

([28]) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità dei sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (Cfr. pag. 27 della presente Gazzetta ufficiale).

c) migliorando la qualità dei dati e armonizzando i requisiti di qualità per i dati conservati nei sistemi di informazione dell'UE, nel rispetto dei requisiti concernenti il trattamento dei dati previsti dagli strumenti giuridici che disciplinano i singoli sistemi e delle norme e dei principi in materia di protezione dei dati;

d) agevolando e sostenendo gli Stati membri nell'attuazione tecnica e operativa dei sistemi di informazione dell'UE;

e) rafforzando, semplificando e rendendo più uniformi le condizioni di sicurezza e protezione dei dati che disciplinano i diversi sistemi di informazione dell'UE, fatte salve la protezione speciale e le garanzie previste per talune categorie di dati;

f) semplificando le condizioni di accesso delle autorità designate all'EES, al VIS, all'ETIAS e all'Eurodac, garantendo al contempo condizioni necessarie e proporzionate per tale accesso;

g) sostenendo le finalità dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e dell'ECRIS-TCN.

Articolo 3

Ambito di applicazione

1. Il presente regolamento si applica all'Eurodac, al SIS e all'ECRIS-TCN.

2. Il presente regolamento si applica ai dati Europol nella misura in cui consente di interrogarli simultaneamente ai sistemi di informazione dell'UE di cui al paragrafo 1.

3. Il presente regolamento si applica alle persone i cui dati personali possono essere trattati nei sistemi di informazione dell'UE di cui al paragrafo 1 e nei dati Europol di cui al paragrafo 2.

Articolo 4

Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

1) «frontiere esterne»: le frontiere esterne quali definite all'articolo 2, punto 2), del regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio ([29]);

2) «verifiche di frontiera»: le verifiche di frontiera quali definite all'articolo 2, punto 11), del regolamento (UE) 2016/399;

3) «autorità di frontiera»: le guardie di frontiera incaricate, conformemente al diritto nazionale, di procedere alle verifiche di frontiera;

4) «autorità di controllo»: l'autorità di controllo di cui all'articolo 51, paragrafo 1, del regolamento (UE) 2016/679 e l'autorità di controllo di cui all'articolo 41, paragrafo 1, della direttiva (UE) 2016/680;

5) «verifica»: il procedimento di confronto di serie di dati al fine di verificare la validità di una identità dichiarata (verifica «uno a uno»);

6) «identificazione»: il procedimento volto a determinare l'identità di una persona mediante interrogazione di una banca dati confrontando varie serie di dati (verifica «uno a molti»);

7) «dati alfanumerici»: i dati rappresentati da lettere, cifre, caratteri speciali, spazi e segni di punteggiatura;

8) «dati di identità»: i dati di cui all'articolo 27, paragrafo 3, lettere da a) a e);

9) «dati relativi alle impronte digitali»: le immagini delle impronte digitali e le immagini delle impronte digitali latenti che, per il loro carattere di unicità e i punti caratteristici che contengono, permettono confronti precisi e irrefutabili sull'identità di una persona;

([29]) 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).

10) «immagine del volto», le immagini digitalizzate del volto di una persona;

11) «dati biometrici»: i dati relativi alle impronte digitali o all'immagine del volto o di entrambe;

12) «template biometrico»: la rappresentazione matematica ottenuta estraendo elementi dai dati biometrici, limitatamente alle caratteristiche necessarie per effettuare identificazioni e verifiche;

13) «documento di viaggio»: il passaporto o altro documento equivalente che autorizza il titolare ad attraversare le frontiere esterne e sul quale può essere apposto un visto;

14) «dati del documento di viaggio»: tipo, numero e paese di rilascio del documento di viaggio, data di scadenza della validità del documento di viaggio e codice a tre lettere del paese di rilascio del documento di viaggio;

15) «sistemi di informazione dell'UE»: l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS e l'ECRIS-TCN;

16) «dati Europol»: i dati personali trattati da Europol per le finalità di cui all'articolo 18, paragrafo 2, lettere da a) a c), del regolamento (UE) 2016/794;

17) «banche dati Interpol»: la banca dati Interpol sui documenti di viaggio rubati o smarriti (banca dati SLTD) e la banca dati Interpol sui documenti di viaggio associati a segnalazioni (banca dati TDAWN);

18) «corrispondenza»: la coincidenza risultante da un confronto automatizzato tra dati personali registrati o in fase di registrazione in un sistema di informazione o in una banca dati;

19) «autorità di polizia»: l'autorità competente quale definita all'articolo 3, punto 7), della direttiva (UE) 2016/680;

20) «autorità designate»: le autorità designate dagli Stati membri, quali definite all'articolo 3, punto 26), del regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio ([30]), all'articolo 2, paragrafo 1, lettera e), della decisione 2008/633/GAI del Consiglio ([31]) e all'articolo 3, paragrafo 1, punto 21), del regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio ([32]);

21) «reato di terrorismo», il reato che, ai sensi del diritto nazionale, corrisponde o è equivalente a uno dei reati di cui alla direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio ([33]);

22) «reato grave»: il reato che corrisponde o è equivalente a uno dei reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio ([34]), se è punibile conformemente al diritto nazionale con una pena detentiva o una misura di sicurezza privativa della libertà personale per un periodo massimo di almeno tre anni;

23) «Sistema di ingressi/uscite» o «EES»: il sistema di ingressi/uscite istituito dal regolamento (UE) 2017/2226;

24) «Sistema di informazione visti» o «VIS»: il sistema di informazione visti istituito dal regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio ([35]);

25) «Sistema europeo di informazione e autorizzazione ai viaggi» o «ETIAS»: il sistema europeo di informazione e autorizzazione ai viaggi istituito dal regolamento (UE) 2018/1240;

([30]) Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011 (GU L 327 del 9.12.2017, pag. 20).

([31]) Decisione 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi (GU L 218 del 13.8.2008, pag. 129).

([32]) Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (GU L 236 del 19.9.2018, pag. 1).

([33]) 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).

([34]) Decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU L 190 del 18.7.2002, pag. 1).

([35]) Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS) (GU L 218 del 13.8.2008, pag. 60).

26) «Eurodac»: l'Eurodac istituito dal regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio ([36]);

27) «Sistema di informazione Schengen» o «SIS»: il sistema d'informazione Schengen istituito dai regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862;

28) «ECRIS-TCN»: il sistema centralizzato per l'identificazione degli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi istituito dal regolamento (UE) 2019/816

Articolo 5

Non discriminazione e diritti fondamentali

Il trattamento di dati personali ai fini del presente regolamento non dà luogo a discriminazioni nei confronti delle persone fondate sul genere, sulla razza, sul colore della pelle o sull'origine etnica o sociale, sulle caratteristiche genetiche, sulla lingua, sulla religione o sulle convinzioni personali, sulle opinioni politiche o di qualsiasi altra natura, sull'appartenenza a una minoranza nazionale, sul patrimonio, sulla nascita, sulla disabilità, sull'età o sull'orientamento sessuale. Esso rispetta pienamente la dignità e l'integrità umana nonché i diritti fondamentali, compreso il diritto al rispetto della vita privata e alla protezione dei dati personali. È prestata particolare attenzione ai minori, alle persone anziane, alle persone con disabilità e alle persone bisognose di protezione internazionale. L'interesse superiore del minore è considerato preminente.

CAPO II

Portale di ricerca europeo

Articolo 6

Portale di ricerca europeo

1. È istituito un portale di ricerca europeo (ESP) al fine di agevolare l'accesso rapido, continuato, efficace, sistematico e controllato delle autorità degli Stati membri e delle agenzie dell'Unione ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol per lo svolgimento dei loro compiti e conformemente ai rispettivi diritti di accesso e agli obiettivi e scopi dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e dell'ECRIS-TCN.

2. L'ESP è composto da:

a) un'infrastruttura centrale, che comprende un portale di ricerca per l'interrogazione simultanea dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS, dell'ECRIS-TCN, dei dati Europol e delle banche dati Interpol;

b) un canale di comunicazione sicuro tra l'ESP, gli Stati membri e le agenzie dell'Unione autorizzati a usare l'ESP;

c) un'infrastruttura di comunicazione sicura tra l'ESP e l'EES, il VIS, l'ETIAS, l'Eurodac, il SIS centrale, l'ECRIS-TCN, i dati Europol e le banche dati Interpol nonché tra l'ESP e le infrastrutture centrali del CIR e del MID.

3. eu-LISA provvede allo sviluppo dell'ESP e ne assicura la gestione tecnica.

Articolo 7

Uso del portale di ricerca europeo

1. L'uso dell'ESP è riservato alle autorità degli Stati membri e alle agenzie dell'Unione che hanno accesso ad almeno uno dei sistemi di informazione dell'UE conformemente agli strumenti giuridici che disciplinano tali sistemi di informazione dell'UE, al CIR e al MID conformemente al presente regolamento, ai dati Europol conformemente al regolamento (UE) 2016/794 e alle banche dati Interpol conformemente al diritto dell'Unione o nazionale che regola tale accesso.

Dette autorità degli Stati membri e agenzie dell'Unione possono ricorrere all'ESP e ai dati che esso fornisce solo per gli obiettivi e le finalità stabiliti dagli strumenti giuridici che disciplinano tali sistemi di informazione dell'UE, nel regolamento (UE) 2016/794 e nel presente regolamento.

([36]) Regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (GU L 180 del 29.6.2013, pag. 1).

2. Le autorità dello Stato membro e le agenzie dell'Unione di cui al paragrafo 1 usano l'ESP per cercare dati relativi a persone o documenti di viaggio nei sistemi centrali dell'Eurodac e dell'ECRIS-TCN, conformemente ai rispettivi diritti di accesso di cui agli strumenti giuridici che disciplinano tali sistemi di informazione dell'UE e al diritto nazionale. Si avvalgono dell'ESP anche per interrogare il CIR, conformemente ai rispettivi diritti di accesso a norma del presente regolamento, ai fini degli articoli 20, 21 e 22.

3. Le autorità degli Stati membri di cui al paragrafo 1 possono usare l'ESP per cercare dati relativi a persone o documenti di viaggio nel SIS centrale di cui ai regolamenti (UE) 2018/1860 e (UE) 2018/1861.

4. Quando previsto a norma del diritto dell'Unione, le agenzie dell'Unione di cui al paragrafo 1 usano l'ESP per cercare nel SIS centrale dati relativi a persone o documenti di viaggio.

5. Le autorità dello Stato membro e le agenzie dell'Unione di cui al paragrafo 1 possono usare l'ESP per cercare dati relativi a persone o documenti di viaggio nei dati Europol, conformemente ai rispettivi diritti di accesso a norma del diritto dell'Unione e nazionale.

Articolo 8

Profili per gli utenti del portale di ricerca europeo

1. Al fine di consentire l'uso dell'ESP, eu-LISA crea, in cooperazione con gli Stati membri, un profilo basato su ciascuna categoria di utenti dell'ESP e sulle finalità delle loro interrogazioni, secondo le modalità tecniche e i diritti di accesso di cui al paragrafo 2. Ogni profilo comprende, conformemente al diritto dell'Unione e nazionale, le seguenti informazioni:

a) i campi di dati da usare per l'interrogazione;

b) i sistemi di informazione dell'UE, i dati Europol e le banche dati Interpol che sono da interrogare, quelli che possono essere interrogati e quelli che devono fornire una risposta all'utente;

c) i dati specifici contenuti nei sistemi di informazione dell'UE, i dati Europol e le banche dati Interpol che possono essere interrogati;

d) le categorie di dati che possono essere forniti in ciascuna risposta.

2. La Commissione adotta atti di esecuzione per specificare le modalità tecniche dei profili di cui al paragrafo 1, nel rispetto dei rispettivi diritti di accesso degli utenti dell'ESP, conformemente agli strumenti giuridici che disciplinano i sistemi di informazione dell'UE e al diritto nazionale. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

3. I profili di cui al paragrafo 1 sono riesaminati periodicamente da eu-LISA in cooperazione con gli Stati membri, almeno una volta all'anno, e aggiornati se necessario.

Articolo 9

Interrogazioni

1. Gli utenti dell'ESP avviano un'interrogazione presentando dati alfanumerici o biometrici all'ESP. Ove un'interrogazione sia stata lanciata, l'ESP interroga simultaneamente l'EES, l'ETIAS, il VIS, il SIS, l'Eurodac, l'ECRIS-TCN, il CIR, i dati Europol e le banche dati Interpol, usando i dati presentati dall'utente e in funzione del profilo dell'utente.

2. Le categorie di dati usati per avviare l'interrogazione tramite l'ESP corrispondono alle categorie di dati relativi a persone o documenti di viaggio che possono essere usati per interrogare i vari sistemi di informazione dell'UE, i dati Europol e le banche dati Interpol conformemente agli strumenti giuridici che li disciplinano.

3. eu-LISA, in cooperazione con gli Stati membri, implementa un documento di controllo dell'interfaccia per l'ESP basato sul formato universale dei messaggi di cui all'articolo 38.

4. Ove un'interrogazione sia stata lanciata da un utente dell'ESP, l'EES, l'ETIAS, il VIS, il SIS, l'Eurodac, l'ECRIS-TCN, il CIR, il MID, i dati Europol e le banche dati Interpol risponde all'interrogazione fornendo i dati in essi contenuti.

Fatto salvo l'articolo 20, la risposta fornita dall'ESP indica il sistema di informazione dell'UE o la banca dati cui appartengono i dati.

L'ESP non fornisce alcuna informazione in merito ai dati contenuti nei sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol a cui l'utente non ha accesso ai sensi del diritto dell'Unione e nazionale applicabile.

5. L'ESP è progettato in modo da garantire che le interrogazioni delle banche dati Interpol lanciate attraverso l'ESP siano effettuate in modo tale che nessuna informazione sia rivelata al titolare della segnalazione Interpol.

6. L'ESP fornisce risposte all'utente non appena i dati sono disponibili in uno dei sistemi di informazione dell'UE, nei dati Europol o nelle banche dati Interpol. Tali risposte contengono unicamente i dati a cui l'utente ha accesso in base al diritto dell'Unione e nazionale.

7. La Commissione adotta un atto di esecuzione per specificare la procedura tecnica di interrogazione da parte dell'ESP dei sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol e il formato delle risposte dell'ESP. Tale atto di esecuzione è adottato secondo la procedura di esame di cui all'articolo 70, paragrafo 2.

Articolo 10

Registrazioni

1. Fatti salvi gli articoli 12 e 18 del regolamento (UE) 2018/1862, l'articolo 29 del regolamento (UE) 2019/816 e l'articolo 40 del regolamento (UE) 2016/794, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nell'ESP. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che effettua l'interrogazione e il profilo ESP usato;

b) la data e l'ora dell'interrogazione;

c) i sistemi di informazione dell'UE e i dati Europol interrogati.

2. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tali autorità debitamente autorizzato a usare l'ESP. Ciascuna agenzia dell'Unione conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi. Dette registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Se, tuttavia, tali registrazioni siano necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando non sono più necessarie per le procedure di monitoraggio.

Articolo 11

Procedure sostitutive in caso di impossibilità tecnica dell'uso del portale di ricerca europeo

1. Qualora sia tecnicamente impossibile usare l'ESP per interrogare uno o più sistemi di informazione dell'UE, o il CIR a causa di un guasto dell'ESP, eu-LISA ne informa i relativi utenti in modo automatizzato.

2. Qualora sia tecnicamente impossibile usare l'ESP per interrogare uno o più sistemi di informazione dell'UE o il CIR a causa di un guasto dell'infrastruttura nazionale di uno Stato membro, tale Stato membro ne informa eu-LISA e la Commissione in modo automatizzato.

3. Nei casi di cui ai paragrafi 1 e 2 del presente articolo, fintantoché il guasto tecnico non è riparato, l'obbligo di cui all'articolo 7, paragrafi 2 e 4, non si applica e gli Stati membri accedono ai sistemi di informazione dell'UE, o al CIR direttamente quando sono tenuti a farlo ai sensi del diritto nazionale o dell'Unione.

4. Qualora sia tecnicamente impossibile usare l'ESP per interrogare uno o più sistemi di informazione dell'UE o il CIR a causa di un guasto dell'infrastruttura di un'agenzia dell'Unione, l'agenzia in questione ne informa eu-LISA e la Commissione in modo automatizzato.

CAPO III

Servizio comune di confronto biometrico

Articolo 12

Servizio comune di confronto biometrico

1. Al fine di sostenere il CIR e il MID nonché gli obiettivi dell'EES, del VIS, dell'Eurodac, del SIS e dell'ECRIS-TCN è istituito un servizio comune di confronto biometrico (BMS comune) che conserva i template biometrici ottenuti dai dati biometrici di cui all'articolo 13 registrati nel CIR e nel SIS e consente di effettuare interrogazioni con dati biometrici trasversalmente in più sistemi di informazione dell'UE.

2. Il BMS comune è composto di:

a) un'infrastruttura centrale, che sostituisce i sistemi centrali rispettivamente dell'EES, del VIS, del SIS, dell'Eurodac e dell'ECRIS-TCN nella misura in cui registri template biometrici e consenta di effettuare ricerche con dati biometrici;

b) un'infrastruttura di comunicazione sicura tra il BMS comune, il SIS centrale e il CIR.

3. eu-LISA provvede allo sviluppo del BMS comune e ne assicura la gestione tecnica.

Articolo 13

Conservazione di template biometrici nel servizio comune di confronto biometrico

1. Il BMS comune conserva i template biometrici che ottiene dai seguenti dati biometrici:

a) i dati di cui all'articolo 20, paragrafo 3, lettere w) e y), esclusi i dati sulle impronte digitali, del regolamento (UE) 2018/1861;

b) i dati di cui all'articolo 5, paragrafo 1, lettera b, e paragrafo 2, del regolamento (UE) 2019/816

I template biometrici devono essere conservati nel BMS comune, separati per logica in base al sistema di informazione dell'UE di provenienza dei dati

2. Per ciascuna serie di dati di cui al paragrafo 1, il BMS comune inserisce in ogni template biometrico un riferimento ai sistemi di informazione dell'UE in cui sono conservati i corrispondenti dati biometrici e un riferimento alla effettiva registrazione nei sistemi di informazione dell'UE.

3. I template biometrici sono inseriti nel BMS comune solo dopo che questo ha effettuato un controllo automatizzato della qualità dei dati biometrici aggiunti in uno dei sistemi di informazione dell'UE al fine di accertare il rispetto di norme minime di qualità dei dati.

4. La conservazione dei dati di cui al paragrafo 1 rispetta le norme di qualità di cui all'articolo 37, paragrafo 2.

5. La Commissione stabilisce, mediante un atto di esecuzione, i requisiti di prestazione e le modalità pratiche per il monitoraggio delle prestazioni del BMS comune, al fine di garantire che l'efficacia delle ricerche biometriche rispetti procedure critiche in termini di tempo quali i controlli di frontiera e le identificazioni. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

Articolo 14

Ricerca di dati biometrici tramite il servizio comune di confronto biometrico

Per la ricerca dei dati biometrici conservati al loro interno, il CIR e il SIS usano i template biometrici conservati nel BMS comune. Le interrogazioni con dati biometrici sono effettuate per le finalità del presente regolamento e dei regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 e (UE) 2019/816.

Articolo 15

Periodo di conservazione dei dati nel servizio comune di confronto biometrico

I dati di cui all'articolo 13, paragrafi 1 e 2, sono conservati nel BMS comune per il tempo in cui i corrispondenti dati biometrici sono conservati nel CIR o nel SIS. I dati sono cancellati dal BMS comune in modo automatizzato.

Articolo 16

Registrazioni

1. Fatti salvi gli articoli 12 e 18 del regolamento (UE) 12/2226 e l'articolo 29 del regolamento (UE) 2019/816, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nel BMS comune. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che ha effettuato l'interrogazione;

b) lo storico della creazione e della conservazione dei template biometrici;

c) i sistemi di informazione dell'UE interrogati con i template biometrici conservati nel BMS comune;

d) la data e l'ora dell'interrogazione;

e) il tipo di dati biometrici usati per avviare l'interrogazione;

f) i risultati dell'interrogazione e la data e l'ora del risultato;

2. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tali autorità debitamente autorizzato a usare il BMS comune. Ciascuna agenzia dell'Unione conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato.

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi ai sensi dell'articolo 42. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Se, tuttavia, tali registrazioni siano necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando non sono più necessarie per le procedure di monitoraggio.

CAPO IV

Archivio comune di dati di identità

Articolo 17

Archivio comune di dati di identità

1. Al fine di agevolare e contribuire alla corretta identificazione delle persone registrate nell'EES, nel VIS, nell'ETIAS, nell'Eurodac e nell'ECRIS-TCN conformemente all'articolo 20, di sostenere il funzionamento del MID conformemente all'articolo 21 e di agevolare e semplificare alle autorità designate e a Europol l'accesso all'EES, al VIS, all'ETIAS e all'EURODAC, quando necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi conformemente all'articolo 22, è istituito un archivio comune di dati di identità (CIR) che, per ciascuna persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nell'ECRIS-TCN, crea un fascicolo individuale contenente i dati di cui all'articolo 18.

2. Il CIR è composto di:

a) un'infrastruttura centrale che sostituisce i sistemi centrali dell'EES, del VIS, dell'ETIAS, dell'Eurodac e dell'ECRIS-TCN, rispettivamente, nella misura in cui conserva i dati di cui all'articolo 18;

b) un canale di comunicazione sicuro tra il CIR, gli Stati membri e le agenzie dell'Unione autorizzate a usare il CIR conformemente al diritto dell'Unione e nazionale;

c) un'infrastruttura di comunicazione sicura tra il CIR e l'EES, il VIS, l'ETIAS, l'Eurodac e l'ECRIS-TCN nonché le infrastrutture centrali dell'ESP, del BMS comune e del MID.

3. eu-LISA provvede allo sviluppo del CIR e ne assicura la gestione tecnica.

4. Qualora, a causa di un guasto del CIR, sia tecnicamente impossibile interrogare tale archivio ai fini dell'identificazione di una persona conformemente all'articolo 20, a fini di individuazione di identità multiple a norma dell'articolo 21 o a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi a norma dell'articolo 22, eu-LISA ne informa i relativi utenti in modo automatizzato.

5. eu-LISA, in cooperazione con gli Stati membri, implementa un documento di controllo dell'interfaccia per il CIR basato sul formato universale dei messaggi di cui all'articolo 38.

Articolo 18

Dati dell'archivio comune di dati di identità

1. Il CIR conserva i seguenti dati, separati per logica in base al sistema di informazione di provenienza dei dati: i dati di cui all'articolo 5, paragrafo 1, lettera b), e paragrafo 2, del regolamento (UE) 2019/816 e i seguenti dati elencati all'articolo 5, paragrafo 1, lettera a), del medesimo regolamento: cognome; nome o nomi; data di nascita; luogo di nascita (città e paese); cittadinanza/e; genere, nomi precedenti, se del caso, ove disponibili pseudonimi, nonché informazioni sui documenti di viaggio, ove disponibili.

2. Per ciascuna serie di dati di cui al paragrafo 1, il CIR inserisce un riferimento ai sistemi di informazione dell'UE cui appartengono i dati.

3. Le autorità che hanno accesso al CIR effettuano tale accesso conformemente ai rispettivi diritti di accesso ai sensi degli strumenti giuridici che disciplinano i sistemi di informazione dell'UE e ai sensi del diritto nazionale e conformemente ai rispettivi diritti di accesso ai sensi del presente regolamento, ai fini di cui agli articoli 20, 21 e 22.

4. Per ciascuna serie di dati di cui al paragrafo 1 il CIR inserisce un riferimento all'effettiva registrazione nei sistemi di informazione dell'UE cui appartengono i dati.

5. La conservazione dei dati di cui al paragrafo 1 rispetta le norme di qualità di cui all'articolo 37, paragrafo 2.

Articolo 19

Aggiunta, modifica e cancellazione di dati nell'archivio comune di dati di identità

1. Qualora nell'Eurodac o nell'ECRIS-TCN siano aggiunti, modificati o cancellati dati, sono aggiunti, modificati o cancellati di conseguenza, in modo automatizzato, i dati di cui all'articolo 18 conservati nel fascicolo individuale del CIR.

2. Qualora sia creato un collegamento bianco o rosso nel MID, conformemente all'articolo 32 o all'articolo 33, tra i dati di due o più sistemi di informazione dell'UE che compongono il CIR, quest'ultimo non crea un nuovo fascicolo individuale, bensì aggiunge i nuovi dati al fascicolo individuale dei dati oggetto del collegamento.

Articolo 20

Accesso all'archivio comune di dati di identità a fini di identificazione

1. Le interrogazioni del CIR sono effettuate da un'autorità di polizia conformemente ai paragrafi 1 e 2 unicamente nei casi seguenti:

a) se l'autorità di polizia non è in grado di identificare una persona in ragione dell'assenza di un documento di viaggio o di un altro documento credibile che ne provi l'identità;

b) se sussistono dubbi quanto ai dati di identità forniti dall'interessato;

c) se sussistono dubbi quanto all'autenticità del documento di viaggio o di un altro documento credibile fornito dall'interessato;

d) se sussistono dubbi quanto all'identità del titolare del documento di viaggio o di un altro documento credibile; ovvero

e) se l'interessato non è in grado o rifiuta di cooperare.

Tali interrogazioni non sono autorizzate nel caso di minori di età inferiore a 12 anni, a meno che ciò non sia nell'interesse superiore del minore.

2. Qualora si verifichi uno dei casi di cui al paragrafo 1, l'autorità di polizia appositamente autorizzata da una misura legislativa nazionale di cui al paragrafo 5 può, unicamente ai fini dell'identificazione di una persona, interrogare il CIR con i dati biometrici dell'interessato acquisiti sul posto durante una verifica d'identità, a condizione che la procedura sia stata avviata in presenza dell'interessato.

3. Se dall'interrogazione risulta che nel CIR sono conservati dati dell'interessato, l'autorità di polizia ha accesso al CIR per consultare i dati di cui all'articolo 18, paragrafo 1.

Se non possono essere usati i dati biometrici dell'interessato o se l'interrogazione con tali dati non dà esito, l'interrogazione è effettuata con i dati di identità dell'interessato combinati con i dati del documento di viaggio oppure con i dati di identità forniti dall'interessato.

4. L'autorità di polizia appositamente autorizzata da una misura legislativa nazionale di cui al paragrafo 6 può, in caso di catastrofe naturale, incidente o attacco terroristico e unicamente ai fini dell'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati, interrogare il CIR con i dati biometrici degli interessati.

5. Gli Stati membri che intendono valersi della possibilità offerta dal paragrafo 2 adottano misure legislative nazionali. Nell'adottare tali misure gli Stati membri tengono conto della necessità di evitare qualsiasi discriminazione nei confronti di cittadini di paesi terzi. Tali misure specificano le finalità esatte dell'identificazione nell'ambito degli obiettivi di cui all'articolo 2, paragrafo 1, lettere b) e c). Designano le autorità di polizia competenti e stabiliscono le procedure, le condizioni e i criteri di tali verifiche.

6. Gli Stati membri che intendono valersi della possibilità offerta dal paragrafo 4 adottano misure legislative nazionali che stabiliscono le procedure, le condizioni e i criteri.

Articolo 21

Accesso all'archivio comune di dati di identità a fini di individuazione di identità multiple

1. Se un'interrogazione del CIR dà luogo a un collegamento giallo conformemente all'articolo 28, paragrafo 4, l'autorità responsabile della verifica manuale delle identità diverse conformemente all'articolo 29 ha accesso, unicamente ai fini della verifica, ai dati di cui all'articolo 18, paragrafi 1 e 2, conservati nel CIR interessati dal collegamento giallo.

2. Se un'interrogazione del CIR dà luogo a un collegamento rosso conformemente all'articolo 32, le autorità di cui all'articolo 26, paragrafo 2, hanno accesso, unicamente al fine di combattere la frode di identità, ai dati di cui all'articolo 18, paragrafi 1 e 2, conservati nel CIR interessati dal collegamento rosso.

Articolo 22

Interrogazione dell'archivio comune di dati di identità a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi

1. Se in un caso specifico vi sono fondati motivi per ritenere che la consultazione dei sistemi di informazione dell'UE contribuisca alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o di altri reati gravi, in particolare laddove sussista il sospetto che i dati dell'autore presunto o effettivo oppure della vittima di reati di terrorismo o di altri reati gravi siano conservati nell'Eurodac, le autorità designate e Europol possono consultare il CIR per sapere se nell'Eurodac sono presenti dati su una determinata persona.

2. Se nell'Eurodac sono presenti dati sulla persona in questione, il CIR risponde all'interrogazione fornendo alle autorità designate e a Europol un riferimento di cui all'articolo 18, paragrafo 2, all'Eurodac che contiene i corrispondenti dati. Il CIR risponde con modalità tali che non compromettano la sicurezza dei dati.

La risposta che indica che i dati sulla persona in questione sono presenti in Eurodac è utilizzata solo per presentare una richiesta di accesso integrale soggetta alle condizioni e alle procedure stabilite dallo strumento giuridico che disciplina tale accesso.

In caso di una o più corrispondenze, l'autorità designata o Europol richiede il pieno accesso ad almeno uno dei sistemi di informazione dai quali è emersa una corrispondenza.

Ove, in via eccezionale, tale accesso integrale non sia richiesto, le autorità designate registrano la motivazione per la mancata richiesta, che deve essere tracciabile nel fascicolo nazionale. Europol registra la motivazione nel pertinente fascicolo.

3. Il pieno accesso ai dati contenuti nell'Eurodac a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi è soggetto alle condizioni e procedure previste nello strumento giuridico che disciplina tale accesso.

Articolo 23

Periodo di conservazione dei dati nell'archivio comune di dati di identità

1. I dati di cui all'articolo 18, paragrafi 1, 2 e 4, sono cancellati in modo automatizzato dal CIR conformemente alle disposizioni in materia di conservazione dei dati del regolamento (UE) 2019/816.

2. Il fascicolo individuale è conservato nel CIR soltanto per il tempo in cui i corrispondenti dati sono conservati in almeno uno dei sistemi di informazione dell'UE i cui dati sono contenuti nel CIR. La creazione di un collegamento non incide sul periodo di conservazione di ciascuno dei singoli dati oggetto del collegamento.

Articolo 24

Registrazioni

1. Fatto salvo l'articolo 29 del regolamento (UE) 2019/816, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nel CIR conformemente ai paragrafi 2, 3 e 4 del presente articolo.

2. eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati ai sensi dell'articolo 20 nel CIR. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che ha avviato l'interrogazione;

b) la finalità dell'accesso dell'utente che effettua l'interrogazione tramite il CIR;

c) la data e l'ora dell'interrogazione;

d) il tipo di dati usati per avviare l'interrogazione;

e) i risultati dell'interrogazione.

3. eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati ai sensi dell'articolo 21 nel CIR. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro o l'agenzia dell'Unione che ha avviato l'interrogazione;

b) la finalità dell'accesso dell'utente che effettua l'interrogazione tramite il CIR;

c) la data e l'ora dell'interrogazione;

d) ove sia creato un collegamento, i dati usati per avviare l'interrogazione e i risultati dell'interrogazione con indicazione del sistema di informazione dell'UE da cui sono stati ottenuti i dati.

4. eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati ai sensi dell'articolo 22 nel CIR. Tali registrazioni comprendono i seguenti elementi:

a) la data e l'ora dell'interrogazione;

b) i dati usati per avviare l'interrogazione;

c) i risultati dell'interrogazione;

d) lo Stato membro o l'agenzia dell'Unione che ha effettuato l'interrogazione del CIR.

Le autorità di controllo competenti, conformemente all'articolo 41 della direttiva (UE) 2016/680, o il garante europeo della protezione dei dati, conformemente all'articolo 43 del regolamento (UE) 2016/794, verificano periodicamente, a intervalli non superiori a sei mesi, le registrazioni dell'accesso per controllare il rispetto delle procedure e delle condizioni di cui all'articolo 22, paragrafi 1 e 2, del presente regolamento.

5. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tali autorità debitamente autorizzato a usare il CIR ai sensi degli articoli 20, 21 e 22. Ciascuna agenzia dell'Unione conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato ai sensi degli articoli 21 e 22.

Inoltre, per qualsiasi accesso al CIR ai sensi dell'articolo 22, ciascuno Stato membro conserva le seguenti registrazioni:

a) il riferimento del fascicolo nazionale;

b) la finalità dell'accesso;

c) conformemente alle disposizioni nazionali, l'identità utente esclusiva del funzionario che ha effettuato l'interrogazione e del funzionario che ha ordinato l'interrogazione.

6. Conformemente al regolamento (UE) 2016/794, per qualsiasi accesso al CIR ai sensi dell'articolo 22 del presente regolamento, Europol conserva le registrazioni dell'identità utente esclusiva del funzionario che ha effettuato l'interrogazione e del funzionario che ha ordinato l'interrogazione.

7. Le registrazioni di cui ai paragrafi da 2 a 6 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Se, tuttavia, tali registrazioni sono necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando le procedure di monitoraggio non necessitano più di tali registrazioni.

8. eu-LISA conserva le registrazioni relative allo storico dei dati nei fascicoli individuali. eu-LISA cancella tali registrazioni, in modo automatizzato, non appena sono cancellati i dati.

CAPO V

Rilevatore di identità multiple

Articolo 25

Rilevatore di identità multiple

1. Al fine di sostenere il funzionamento del CIR e gli obiettivi dell'EES, del VIS, dell'ETIAS, dell'Eurodac, del SIS e del sistema ECRIS-TCN è istituito un rilevatore di identità multiple (MID) che crea e conserva un fascicolo di conferma dell'identità, ai sensi dell'articolo 34, contenente collegamenti tra i dati dei sistemi di informazione dell'UE inclusi nel CIR e i dati del SIS e che consente il rilevamento delle identità multiple, al duplice scopo di agevolare le verifiche di identità e contrastare la frode di identità.

2. Il MID è composto di:

a) un'infrastruttura centrale che conserva i collegamenti e i riferimenti ai sistemi di informazione dell'UE;

b) un'infrastruttura di comunicazione sicura che collega il MID al SIS e alle infrastrutture centrali dell'ESP e del CIR.

3. eu-LISA provvede allo sviluppo del MID e ne assicura la gestione tecnica.

Articolo 26

Accesso al rilevatore di identità multiple

1. Ai fini della verifica manuale delle identità diverse di cui all'articolo 29, l'accesso ai dati di cui all'articolo 34 conservati nel MID è concesso:

a) all'ufficio SIRENE degli Stati membri che creano o aggiornano una segnalazione conformemente al regolamento (UE) 2018/1862;

b) all'autorità centrale dello Stato membro di condanna quando registra o modifica dati nell'ECRIS-TCN conformemente all'articolo 5 o all'articolo 9 del regolamento (UE) 2019/816.

2. Le autorità degli Stati membri e le agenzie dell'Unione che hanno accesso ad almeno uno dei sistemi di informazione dell'UE inclusi nel CIR o al SIS hanno accesso ai dati di cui all'articolo 34, lettere a) e b), riguardanti i collegamenti rossi di cui all'articolo 32.

3. Le autorità degli Stati membri e le agenzie dell'Unione hanno accesso ai collegamenti bianchi di cui all'articolo 33 se hanno accesso ai due sistemi di informazione dell'UE che contengono dati tra i quali è stato creato il collegamento bianco.

4. Le autorità degli Stati membri e le agenzie dell'Unione hanno accesso ai collegamenti verdi di cui all'articolo 31 se hanno accesso ai due sistemi di informazione dell'UE che contengono dati tra i quali è stato creato il collegamento verde e se dall'interrogazione di tali sistemi di informazione è emersa una corrispondenza tra le due serie di dati oggetto del collegamento.

Articolo 27

Rilevazione di identità multiple

1. È avviata una procedura di rilevazione di identità multiple nel CIR e nel SIS quando:

a) è creata o aggiornata una segnalazione su una persona nel SIS conformemente ai capi da VI a IX del regolamento (UE) 2018/1862;

b) è creata o modificata una registrazione di dati nell'ECRIS-TCN conformemente all'articolo 5 del regolamento (UE) 2019/816.

2. Se tra i dati di un sistema di informazione dell'UE di cui al paragrafo 1 figurano dati biometrici, il CIR e il SIS centrale effettuano la procedura di rilevazione delle identità multiple tramite il BMS comune. Il servizio comune di confronto biometrico raffronta i template biometrici ricavati dai nuovi dati biometrici con i template biometrici già presenti al suo interno e verifica se nel CIR o nel SIS centrale siano già conservati dati della stessa persona.

3. Oltre alla procedura di cui al paragrafo 2, il CIR e il SIS centrale effettuano la ricerca nei dati conservati, rispettivamente, nel CIR e nel SIS centrale mediante l'ESP usando i seguenti dati:

a) cognomi; nomi; nomi e cognomi alla nascita, eventuali nomi e cognomi precedenti e «alias»; luogo di nascita, data di nascita, genere e ogni cittadinanza posseduta, conformemente all'articolo 20, paragrafo 3, del regolamento (UE) 2018/1862;

b) cognome; nome o nomi; data di nascita, luogo di nascita, luogo di nascita (città e paese), cittadinanza o cittadinanze e genere, conformemente all'articolo 5, paragrafo 1, del regolamento (UE) 2019/816.

4. Oltre alla procedura di cui ai paragrafi 2 e 3, il CIR e il SIS centrale effettuano la ricerca nei dati conservati, rispettivamente, nel CIR e nel SIS centrale mediante l'ESP usando i dati del documento di viaggio.

5. La procedura di rilevazione di identità multiple è avviata unicamente per confrontare i dati disponibili in un sistema di informazione dell'UE con i dati disponibili negli altri sistemi di informazione dell'UE.

Articolo 28

Esito della procedura di rilevazione di identità multiple

1. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, non risulti alcuna corrispondenza, le procedure di cui all'articolo 27, paragrafo 1, proseguono conformemente agli strumenti giuridici che le disciplinano.

2. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, risultino una o più corrispondenze, il CIR e, se del caso, il SIS creano un collegamento tra i dati usati per avviare l'interrogazione e i dati per i quali è emersa la corrispondenza.

Qualora risultino più corrispondenze è creato un collegamento tra tutti i dati per i quali è emersa una corrispondenza. Se i dati erano già oggetto di un collegamento, questo è esteso ai dati usati per avviare l'interrogazione.

3. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, risultino una o più corrispondenze e i dati di identità dei fascicoli oggetto del collegamento siano gli stessi o simili, è creato un collegamento bianco conformemente all'articolo 33.

4. Qualora dall'interrogazione di cui all'articolo 27, paragrafi 2, 3 e 4, risultino una o più corrispondenze e i dati di identità dei fascicoli oggetto del collegamento non possano essere considerati simili, è creato un collegamento giallo conformemente all'articolo 30 e si applica la procedura di cui all'articolo 29.

5. La Commissione adotta atti delegati conformemente all'articolo 69 per stabilire le procedure per determinare i casi in cui è possibile considerare che i dati di identità sono identici o simili.

6. I collegamenti sono conservati nel fascicolo di conferma dell'identità di cui all'articolo 34.

7. La Commissione, in collaborazione con eu-LISA, stabilisce con atti di esecuzione le norme tecniche per creare i collegamenti tra i dati di diversi sistemi di informazione dell'UE. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

Articolo 29

Verifica manuale delle identità diverse e autorità responsabili

1. Fatto salvo il paragrafo 2, l'autorità responsabile della verifica manuale delle identità diverse è:

a) l'ufficio SIRENE degli Stati membri, per le corrispondenze emerse durante la creazione o l'aggiornamento di una segnalazione SIS conformemente al regolamento (UE) 2018/1862;

b) l'autorità centrale dello Stato membro di condanna, per le corrispondenze emerse durante la registrazione o la modifica dei dati nell'ECRIS-TCN conformemente all'articolo 5 o all'articolo 9 del regolamento (UE) 2019/816.

Il MID indica l'autorità responsabile della verifica manuale delle identità diverse nel fascicolo di conferma dell'identità.

2. L'autorità responsabile della verifica manuale delle identità diverse nel fascicolo di conferma dell'identità è l'ufficio SIRENE dello Stato membro che ha creato la segnalazione qualora sia creato un collegamento ai dati contenuti in una segnalazione:

a) di persone ricercate per l'arresto a fini di consegna o di estradizione di cui all'articolo 26 del regolamento (UE) 2018/1862;

b) di persone scomparse o vulnerabili di cui all'articolo 32 del regolamento (UE) 2018/1862;

c) di persone ricercate per presenziare a un procedimento giudiziario di cui all'articolo 34 del regolamento (UE) 2018/1862;

d) di persone ai fini di controlli discreti, controlli di indagine o controlli specifici di cui all'articolo 36 del regolamento (UE) 2018/1862.

3. L'autorità responsabile della verifica manuale delle identità diverse ha accesso ai dati oggetto di collegamento contenuti nel pertinente fascicolo di conferma dell'identità e ai dati di identità oggetto del collegamento nel CIR e, se del caso, nel SIS. Essa esamina senza indugio le identità diverse. Una volta completata tale valutazione, l'autorità responsabile aggiorna il collegamento conformemente agli articoli 31, 32 e 33 e lo aggiunge senza indugio al fascicolo di conferma dell'identità.

4. Qualora sia creato più di un collegamento, l'autorità responsabile della verifica manuale delle identità diverse esamina ogni collegamento separatamente.

5. Se i dati per i quali risulta una corrispondenza erano già oggetto di un collegamento, l'autorità responsabile della verifica manuale delle identità diverse valuta la creazione di nuovi collegamenti tenendo conto dei collegamenti esistenti.

Articolo 30

Collegamento giallo

1. Qualora non abbia avuto luogo alcuna verifica manuale dell'identità diversa, il collegamento tra dati di due o più sistemi di informazione dell'UE è classificato giallo nei seguenti casi:

a) il collegamento evidenzia gli stessi dati biometrici ma ha dati di identità simili o differenti;

b) il collegamento evidenzia dati di identità differenti ma condivide gli stessi dati del documento di viaggio e almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici della persona in questione;

c) il collegamento evidenzia gli stessi dati di identità ma ha dati biometrici differenti;

d) il collegamento ha dati di identità simili o differenti ed evidenzia gli stessi dati del documento di viaggio, ma ha dati biometrici differenti.

2. Quando un collegamento è classificato giallo conformemente al paragrafo 1 si applica la procedura di cui all'articolo 29.

Articolo 31

Collegamento verde

1. Il collegamento tra dati di due o più sistemi di informazione dell'UE è classificato verde quando:

a) il collegamento ha dati biometrici differenti ma evidenzia gli stessi dati di identità e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse;

b) il collegamento ha dati biometrici differenti, dati di identità simili o differenti ed evidenzia lo stesso documento di viaggio e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse;

c) il collegamento ha dati di identità differenti ma evidenzia lo stesso documento di viaggio, almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici sulla persona in questione e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse.

2. Quando è interrogato il CIR o il SIS e sussiste un collegamento verde tra due o più sistemi di informazione dell'UE, il MID indica che i dati di identità oggetto del collegamento non si riferiscono alla stessa persona.

3. Se l'autorità di uno Stato membro dispone di prove indicanti che un collegamento verde è stato registrato incorrettamente nel MID, che non è aggiornato o che i dati sono stati trattati nel MID o nei sistemi di informazione dell'UE in violazione del presente regolamento, essa controlla i dati pertinenti conservati nel CIR e nel SIS e, se necessario, rettifica o cancella senza indugio il collegamento dal MID. L'autorità dello Stato membro informa senza indugio lo Stato membro responsabile della verifica manuale delle identità diverse.

Articolo 32

Collegamento rosso

1. Il collegamento tra dati di due o più sistemi di informazione dell'UE è classificato rosso nei seguenti casi:

a) il collegamento evidenzia gli stessi dati biometrici ma ha dati di identità simili o differenti e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono alla stessa persona che usa in maniera ingiustificata le identità in questione;

b) il collegamento evidenzia dati di identità identici, simili o differenti e lo stesso documento di viaggio ma dati biometrici differenti e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse, almeno una delle quali usa in maniera ingiustificata lo stesso documento di viaggio;

c) il collegamento evidenzia gli stessi dati di identità ma dati biometrici differenti e i dati relativi al documento di viaggio sono differenti o assenti, e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse che usano le identità in questione in maniera ingiustificata;

d) il collegamento evidenzia gli stessi dati di identità e lo stesso documento di viaggio, almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici sulla persona in questione e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono alla stessa persona che usa le identità in questione in maniera ingiustificata.

2. Quando è interrogato il CIR o il SIS e sussiste un collegamento rosso tra due o più sistemi di informazione dell'UE, il MID indica i dati di cui all'articolo 34. Al collegamento rosso è dato seguito conformemente al diritto dell'Unione e nazionale, con ogni conseguenza giuridica per la persona in questione essendo basato solamente sui dati pertinenti relativi a tale persona. Dalla mera esistenza di un collegamento rosso non deriva alcuna conseguenza giuridica per la persona in questione.

3. Qualora sia creato un collegamento rosso tra dati dell'EES, del VIS, dell'ETIAS, dell'Eurodac o dell'ECRIS-TCN, il fascicolo individuale conservato nel CIR è aggiornato conformemente all'articolo 19, paragrafo 2.

4. Fatte salve le disposizioni relative al trattamento delle segnalazioni nel SIS di cui ai regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862 e le limitazioni necessarie per proteggere la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non saranno compromesse indagini nazionali, qualora sia creato un collegamento rosso l'autorità responsabile della verifica manuale delle identità diverse informa la persona interessata della presenza di dati di identità multipli illeciti e fornisce alla persona un numero di identificazione unico come indicato all'articolo 34, lettera c), del presente regolamento un riferimento all'autorità responsabile della verifica manuale delle identità diverse come indicato all'articolo 34, lettera d), del presente regolamento, e l'indirizzo del sito web del portale in conformità dell'articolo 49 del presente regolamento.

5. L'informazione di cui al paragrafo 4 è fornita per iscritto mediante un modulo standard dall'autorità responsabile della verifica manuale delle identità diverse. La Commissione determina il contenuto e la presentazione del modulo mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

6. Qualora sia creato un collegamento rosso il MID informa in modo automatizzato le autorità responsabili dei dati oggetto del collegamento.

7. Se un'autorità di uno Stato membro o un'agenzia dell'Unione che ha accesso al CIR o al SIS ha prove che suggeriscono che un collegamento rosso è stato registrato incorrettamente nel MID o che i dati sono stati trattati in nel MID, nel CIR o nel SIS in violazione del presente regolamento, tale autorità o agenzia verifica i dati pertinenti conservati nel CIR e nel SIS e:

a) laddove il collegamento si riferisca a una delle segnalazioni nel SIS di cui all'articolo 29, paragrafo 2, informa immediatamente il competente ufficio SIRENE dello Stato membro che ha creato la segnalazione.

b) in tutti gli altri casi, rettifica o cancella immediatamente il collegamento dal MID.

Se un ufficio SIRENE è contattato ai sensi della lettera a) del primo comma, esso verifica le prove fornite dall'autorità dello Stato membro o dell'agenzia dell'Unione e, se del caso, rettifica o cancella immediatamente il collegamento dal MID.

L'autorità dello Stato membro che ottiene le prove informa senza indugio l'autorità dello Stato membro competente della verifica manuale delle identità diverse di ogni eventuale rettifica o cancellazione di un collegamento rosso.

Articolo 33

Collegamento bianco

1. Il collegamento tra dati di due o più sistemi di informazione dell'UE è classificato bianco nei seguenti casi:

a) il collegamento evidenzia gli stessi dati biometrici e dati di identità identici o simili;

b) il collegamento evidenzia dati di identità identici o simili, gli stessi dati relativi al documento di viaggio e almeno uno dei sistemi di informazione dell'UE non contiene dati biometrici della persona in questione;

c) il collegamento evidenzia gli stessi dati biometrici, gli stessi dati relativi al documento di viaggio ma dati di identità simili;

d) il collegamento evidenzia gli stessi dati biometrici ma dati di identità simili o differenti e l'autorità responsabile della verifica manuale delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a una stessa persona in maniera ingiustificata.

2. Quando è interrogato il CIR o il SIS e sussiste un collegamento bianco tra due sistemi di informazione dell'UE, il MID indica che i dati di identità oggetto del collegamento si riferiscono alla stessa persona Se l'autorità che ha avviato l'interrogazione ha accesso ai dati oggetto del collegamento in base al diritto dell'Unione o nazionale, i sistemi di informazione dell'UE interrogati rispondono indicando, se del caso, tutti i dati oggetto del collegamento riguardanti la persona, facendo così emergere una corrispondenza con i dati oggetto del collegamento bianco.

3. Qualora sia creato un collegamento bianco tra dati nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nell'ECRIS-TCN, il fascicolo individuale conservato nel CIR è aggiornato conformemente all'articolo 19, paragrafo 2.

4. Fatte salve le disposizioni relative al trattamento delle segnalazioni nel SIS contenute nei regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862, e fatte salve le limitazioni necessarie per proteggere la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non siano compromesse indagini nazionali, qualora sia creato un collegamento bianco a seguito di una verifica manuale delle identità diverse, l'autorità responsabile della verifica manuale delle identità diverse informa la persona interessata della presenza di dati di identità simili o diversi e fornisce alla persona un numero di identificazione unico come indicato all'articolo 34, lettera c), del presente regolamento, e mette un riferimento all'autorità manuale responsabile della verifica delle identità diverse come indicato all'articolo 34, lettera d), del presente regolamento, e l'indirizzo del sito web del portale in conformità dell'articolo 49 del presente regolamento.

5. Se un'autorità di uno Stato membro dispone di prove indicanti che un collegamento bianco è stato incorrettamente registrato nel MID, non è aggiornato o che i dati sono stati trattati nel MID o nei sistemi di informazione dell'UE in violazione del presente regolamento, essa controlla i dati pertinenti conservati nel CIR e nel SIS e, se necessario, rettifica o cancella senza indugio il collegamento dal MID. L'autorità dello Stato membro informa senza indugio lo Stato membro responsabile della verifica manuale delle identità diverse.

6. L'informazione di cui al paragrafo 4 è fornita per iscritto mediante un modulo standard dall'autorità responsabile della verifica manuale delle identità diverse. La Commissione determina il contenuto e la presentazione del modulo mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

Articolo 34

Fascicolo di conferma dell'identità

Il fascicolo di conferma dell'identità contiene i seguenti dati:

a) i collegamenti conformemente agli articoli da 30 a 33;

b) un riferimento ai sistemi di informazione dell'UE in cui sono conservati i dati oggetto del collegamento;

c) un numero di identificazione unico che permette di estrarre i dati oggetto del collegamento dai corrispondenti sistemi di informazione dell'UE;

d) l'autorità responsabile della verifica manuale delle identità diverse;

e) la data della creazione del link o di un suo aggiornamento.

Articolo 35

Conservazione dei dati nel rilevatore di identità multiple

I fascicoli di conferma dell'identità e i relativi dati, compresi i collegamenti, sono conservati nel MID solo per il tempo in cui i dati oggetto del collegamento sono conservati in due o più sistemi di informazione dell'UE. Essi sono cancellati dal MID in maniera automatizzata.

Articolo 36

Registrazioni

1. eu-LISA conserva le registrazioni di tutti i trattamenti di dati nel MID. Tali registrazioni comprendono i seguenti elementi:

a) lo Stato membro che ha avviato l'interrogazione;

b) la finalità dell'accesso dell'utente;

c) la data e l'ora dell'interrogazione;

d) il tipo di dati usati per avviare la o le interrogazioni;

e) il riferimento ai dati oggetto del collegamento;

f) lo storico del fascicolo di conferma dell'identità.

2. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità e dal personale di tali autorità debitamente autorizzato a usare il MID. Ciascuna agenzia conserva le registrazioni effettuate dal proprio personale debitamente autorizzato.

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Se tuttavia, tali registrazioni siano necessarie per procedure di monitoraggio già avviate, esse sono cancellate quando le procedure di monitoraggio non necessitano più delle registrazioni.

CAPO VI

Misure a sostegno dell'interoperabilità

Articolo 37

Qualità dei dati

1. Fatta salva responsabilità degli Stati membri per quanto riguarda la qualità dei dati inseriti nei sistemi, eu-LISA istituisce procedure e meccanismi automatizzati di controllo della qualità dei dati per i dati conservati nel SIS, nell'Eurodac, nell'ECRIS-TCN, nel BMS comune e nel CIR.

2. eu-LISA applica meccanismi per la valutazione della precisione del BMS comune, istituisce indicatori comuni della qualità dei dati e norme minime di qualità per conservare i dati nel SIS, nell'Eurodac, nell'ECRIS-TCN, nel BMS comune e nel CIR.

Solo i dati che rispettano le norme minime di qualità possono essere inseriti nel SIS, nell'Eurodac, nell'ECRIS-TCN, nel BMS comune, nel CIR e nel MID.

3. eu-LISA riferisce periodicamente agli Stati membri in merito alle procedure e ai meccanismi automatizzati di controllo della qualità dei dati e agli indicatori comuni della qualità dei dati. eu-LISA riferisce periodicamente alla Commissione in merito ai problemi incontrati e agli Stati membri interessati. Su richiesta, eu-LISA presenta tale relazione anche al Parlamento europeo e al Consiglio. Nessuna delle relazioni di cui al presente paragrafo contiene dati personali.

4. I dettagli delle procedure e dei meccanismi automatizzati di controllo della qualità dei dati, gli indicatori comuni della qualità dei dati e le norme minime di qualità per conservare i dati nel SIS, nell'Eurodac, nell'ECRIS-TCN, nel BMS comune e nel CIR, in particolare per quanto riguarda i dati biometrici, sono stabiliti in atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

5. Un anno dopo l'istituzione delle procedure e dei meccanismi automatizzati di controllo della qualità dei dati, degli indicatori comuni della qualità dei dati e delle norme minime di qualità dei dati, e successivamente ogni anno, la Commissione valuta l'attuazione da parte degli Stati membri dei requisiti di qualità dei dati e formula le eventuali raccomandazioni necessarie. Gli Stati membri presentano alla Commissione un piano d'azione volto a correggere le carenze riscontrate nella relazione di valutazione e, in particolare, i problemi relativi alla qualità dei dati derivanti da dati errati nei sistemi di informazione dell'UE. Gli Stati membri riferiscono regolarmente alla Commissione sui progressi compiuti con il piano d'azione fino alla sua completa attuazione.

La Commissione trasmette la relazione di valutazione al Parlamento europeo, al Consiglio, al garante europeo della protezione dei dati, al Comitato europeo per la protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali istituita con regolamento (CE) n. 168/2007 del Consiglio ([37]).

Articolo 38

Formato universale dei messaggi

1. È istituito lo standard del formato universale dei messaggi (UMF). Lo standard UMF definisce le norme relative a determinati elementi relativi al contenuto dello scambio di informazioni transfrontaliero tra i sistemi di informazione, le autorità e/o le organizzazioni del settore Giustizia e affari interni.

([37]) Regolamento (CE) n. 168/2007 del Consiglio, del 15 febbraio 2007, che istituisce l'Agenzia dell'Unione europea per i diritti fondamentali (GU L 53 del 22.2.2007, pag. 1).

2. Lo standard UMF è usato per lo sviluppo dell'Eurodac, dell'ECRIS-TCN, dell'ESP, del CIR, del MID e, se del caso, per lo sviluppo da parte di eu-LISA o di altra agenzia dell'UE di nuovi modelli per lo scambio di informazioni o nuovi sistemi di informazione del settore Giustizia e affari interni.

3. Ai fini dell'istituzione e dello sviluppo dello standard UMF di cui al paragrafo 1 del presente articolo, la Commissione adotta un atto di esecuzione. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

Articolo 39

Archivio centrale di relazioni e statistiche

1. È istituito un archivio centrale di relazioni e statistiche (CRRS) al fine di sostenere gli obiettivi del SIS, dell'Eurodac e dell'ECRIS-TCN, in conformità dei rispettivi strumenti giuridici che disciplinano tali sistemi, e fornire dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati.

2. eu-LISA istituisce, attua e ospita il CRRS nei suoi siti tecnici contenenti, separati per logica in base al sistema di informazione dell'UE, i dati e le statistiche di cui all'articolo 74 del regolamento (UE) 2018/1862 e all'articolo 32 del regolamento (UE) 2019/816 L'accesso al CRRS è concesso mediante un accesso sicuro controllato e specifici profili di utente, unicamente ai fini dell'elaborazione di relazioni e statistiche, alle autorità di cui all'articolo 74 del regolamento (UE) 2018/1862 e all'articolo 32 del regolamento (UE) 2019/816.

3. eu-LISA anonimizza i dati e registra i dati anonimizzati nel CRRS. Il processo di anonimizzazione dei dati è automatizzato.

I dati contenuti nel CRRS non consentono l'identificazione delle persone fisiche.

4. Il CRRS è composto di:

a) strumenti necessari per anonimizzare i dati;

b) un'infrastruttura centrale, costituita da un archivio di dati anonimi;

c) un'infrastruttura di comunicazione sicura per collegare il CRRS al SIS, all'Eurodac e all'ECRIS-TCN, nonché alle infrastrutture centrali del BMS comune, del CIR e del MID.

5. La Commissione adotta un atto delegato a norma dell'articolo 69 che stabilisce le modalità di funzionamento del CRRS, comprese le garanzie specifiche per il trattamento dei dati personali a norma dei paragrafi 2 e 3 del presente articolo e le norme di sicurezza applicabili all'archivio.

CAPO VII

Protezione dei dati

Articolo 40

Titolare del trattamento

1. Per quanto riguarda il trattamento dei dati nel BMS comune, le autorità degli Stati membri titolari del trattamento per l'Eurodac, il SIS e l'ECRIS-TCN, rispettivamente, sono titolari del trattamento ai sensi dell'articolo 4, punto 7), del regolamento (UE) 2016/679 o dell'articolo 3, punto 8), della direttiva (UE) 2016/680 in relazione ai template biometrici ottenuti dai dati di cui all'articolo 13 del presente regolamento inseriti da ciascuna autorità nel rispettivo sistema e hanno la responsabilità del trattamento dei template biometrici nel BMS comune.

2. Per quanto riguarda il trattamento dei dati nel CIR, le autorità degli Stati membri titolari del trattamento per l'Eurodac e l'ECRIS-TCN, rispettivamente, sono titolari del trattamento ai sensi dell'articolo 4, punto 7), del regolamento (UE) 2016/679 o dell'articolo 3, punto 8), della direttiva (UE) 2016/680 in relazione ai dati di cui all'articolo 18 del presente regolamento inseriti da ciascuna autorità nel rispettivo sistema e hanno la responsabilità del trattamento di tali dati personali nel CIR.

3. Per quanto riguarda il trattamento dei dati nel MID:

a) l'Agenzia europea della guardia di frontiera e costiera è responsabile del trattamento ai sensi dell'articolo 3, punto 8), del regolamento (UE) 2018/1725 in relazione al trattamento di dati personali da parte dell'unità centrale ETIAS;

b) le autorità degli Stati membri che aggiungono o modificano dati nel fascicolo di conferma dell'identità sono titolari del trattamento ai sensi dell'articolo 4, punto 7), del regolamento (UE) 2016/679 o dell'articolo 3, punto 8), della direttiva (UE) 2016/680 e hanno la responsabilità del trattamento dei dati personali nel MID.

4. Per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, i titolari del trattamento hanno accesso alle registrazioni di cui agli articoli 10, 16, 24 e 36 per la verifica interna di cui all'articolo 44.

Articolo 41

Responsabile del trattamento

Per quanto riguarda il trattamento dei dati personali nel BMS comune, nel CIR e nel MID, eu-LISA è incaricato del trattamento ai sensi dell'articolo 3, punto 12), lettera a), del regolamento (UE) 2018/1725.

Articolo 42

Sicurezza del trattamento

1. eu-LISA, l'unità centrale ETIAS, Europol e le autorità degli Stati membri garantiscono la sicurezza del trattamento di dati personali svolto ai sensi del presente regolamento. eu-LISA, l'unità centrale ETIAS, Europol e le autorità degli Stati membri cooperano nei compiti relativi alla sicurezza.

2. Fatto salvo l'articolo 33 del regolamento (UE) 2018/1725, eu-LISA adotta le misure necessarie per garantire la sicurezza delle componenti dell'interoperabilità e delle relative infrastrutture di comunicazione.

3. In particolare 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, al fine di:

a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani d'emergenza per la protezione delle infrastrutture critiche;

b) negare alle persone non autorizzate l'accesso alle attrezzature e alle strutture utilizzate per il trattamento di dati;

c) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate;

d) impedire che i dati siano inseriti senza autorizzazione e che i dati personali registrati siano visionati, modificati o cancellati senza autorizzazione;

e) impedire che i dati siano trattati, copiati, modificati o cancellati senza autorizzazione;

f) impedire che persone non autorizzate usino sistemi di trattamento automatizzato di dati servendosi di attrezzature per la comunicazione di dati;

g) garantire che le persone autorizzate ad accedere alle componenti dell'interoperabilità abbiano accesso solo ai dati previsti dalla loro autorizzazione di accesso, tramite identità di utente individuali ed esclusivamente con modalità di accesso riservato;

h) garantire che sia possibile verificare e stabilire a quali organismi possono essere trasmessi dati personali mediante apparecchiature di comunicazione dei dati;

i) garantire che sia possibile verificare e stabilire quali dati sono stati trattati nelle componenti dell'interoperabilità, quando, da chi e per quale finalità;

j) impedire, in particolare mediante tecniche appropriate di cifratura, che, all'atto della trasmissione di dati personali dalle componenti dell'interoperabilità o verso le medesime ovvero durante il trasporto dei supporti di dati, tali dati personali vengano letti, copiati, modificati o cancellati senza autorizzazione;

k) garantire che, in caso di interruzione, i sistemi installati possano essere ripristinati;

l) garantire l'affidabilità, accertandosi che eventuali anomalie nel funzionamento delle componenti dell'interoperabilità siano adeguatamente segnalate;

m) 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 e valutare le misure di sicurezza alla luce dei nuovi sviluppi tecnologici.

4. Gli Stati membri, Europol e l'unità centrale ETIAS adottano misure equivalenti a quelle del paragrafo 3 per quanto riguarda la sicurezza del trattamento dei dati personali da parte delle autorità con diritto di accesso a una o più componenti dell'interoperabilità.

Articolo 43

Incidenti di sicurezza

1. È considerato incidente di sicurezza l'evento che ha o può avere ripercussioni sulla sicurezza delle componenti dell'interoperabilità e può causare danni o perdite ai dati ivi conservati, in particolare quando possono essere stati consultati dati senza autorizzazione o quando sono state o possono essere state compromesse la disponibilità, l'integrità e la riservatezza dei dati.

2. Ogni incidente di sicurezza è gestito in modo 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, dell'articolo 30 della direttiva (UE) 2016/680, o di entrambi, gli Stati membri notificano senza indugio qualsiasi incidente di sicurezza alla Commissione, a eu-LISA, alle autorità di controllo competenti e al garante europeo della protezione dei dati

Fatti salvi gli articoli 34 e 35 del regolamento (UE) 2018/1725 e l'articolo 34 del regolamento (UE) 2016/794, l'unità centrale ETIAS ed Europol notificano senza indugio qualsiasi incidente di sicurezza alla Commissione, a eu-LISA e al garante europeo della protezione dei dati.

Qualora si verifichi un incidente di sicurezza in relazione all'infrastruttura centrale delle componenti dell'interoperabilità, eu-LISA ne dà immediatamente notifica alla Commissione e al garante europeo della protezione dei dati.

4. Le informazioni sull'incidente di sicurezza che ha o può avere ripercussioni sul funzionamento delle componenti dell'interoperabilità o sulla disponibilità, integrità e riservatezza dei dati sono fornite senza indugio agli Stati membri, all'unità centrale ETIAS e a Europol e registrate secondo il piano di gestione degli incidenti stabilito da eu-LISA.

5. Gli Stati membri interessati, l'unità centrale ETIAS, Europol ed eu-LISA cooperano in caso di incidente di sicurezza. La Commissione stabilisce con atti di esecuzione le modalità di tale procedura di cooperazione. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 70, paragrafo 2.

Articolo 44

Verifica interna

Gli Stati membri e le pertinenti agenzie dell'Unione provvedono affinché ciascuna autorità con diritto di accesso alle componenti dell'interoperabilità adotti le misure necessarie per verificare la propria conformità al presente regolamento e cooperi, se necessario, con l'autorità di controllo.

I titolari del trattamento di cui all'articolo 40 adottano le misure necessarie per verificare la conformità del trattamento dei dati a norma del presente regolamento, anche attraverso la verifica frequente delle registrazioni di cui agli articoli 10, 16, 24 e 36, e cooperare, laddove necessario, con le autorità di controllo e con il garante europeo della protezione dei dati.

Articolo 45

Sanzioni

Gli Stati membri provvedono affinché qualsiasi uso improprio, trattamento o scambio di dati in contrasto con il presente regolamento sia punibile ai sensi della legislazione nazionale. Le sanzioni previste sono effettive, proporzionate e dissuasive.

Articolo 46

Responsabilità

1. Fatti salvi il diritto al risarcimento e la responsabilità da parte del titolare del trattamento o del responsabile del trattamento ai sensi del regolamento (UE) 2016/679, della direttiva (UE) 2016/680 e del regolamento (UE) 2018/1725:

a) ogni persona o Stato membro che abbia subito danni materiali o immateriali in conseguenza di un trattamento illecito di dati personali 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;

b) ogni persona o Stato membro che abbia subito danni materiali o immateriali in conseguenza di qualsiasi atto incompatibile con il presente regolamento compiuto da Europol, dall'Agenzia europea della guardia di frontiera e costiera o da eu-LISA, ha diritto al risarcimento da parte dell'agenzia in questione.

Lo Stato membro interessato, Europol, l'Agenzia europea della guardia di frontiera e costiera o eu-LISA sono esonerati, in tutto o in parte, dalla responsabilità a norma del primo comma se provano che l'evento dannoso non è loro imputabile.

2. Uno Stato membro è responsabile di ogni eventuale danno arrecato alle componenti dell'interoperabilità conseguente all'inosservanza degli obblighi del presente regolamento, a meno che e nella misura in cui eu-LISA o un altro Stato membro vincolato al presente regolamento abbia omesso di adottare provvedimenti ragionevolmente idonei a prevenire il danno o ridurne al minimo l'impatto.

3. Le azioni proposte nei confronti di uno Stato membro per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono disciplinate dal diritto nazionale dello Stato membro convenuto. Le azioni proposte nei confronti del titolare del trattamento o eu-LISA per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono soggette alle condizioni previste dai trattati.

Articolo 47

Diritto di informazione

1. L'autorità che raccoglie i dati personali da conservare nel BMS comune, nel CIR o nel MID fornisce alle persone i cui dati sono raccolti con le informazioni di cui agli articoli 13 e 14 del regolamento (UE) 2016/679, agli articoli 12 e 13 della direttiva (UE) 2016/680 e agli articoli 15 e 16 del regolamento (UE) 2018/1725. L'autorità fornisce le informazioni al momento della raccolta di tali dati.

2. Tutte le informazioni sono messe a disposizione utilizzando un linguaggio chiaro e semplice, in una versione linguistica comprensibile all'interessato o che ragionevolmente si suppone a lui comprensibile. Ciò comprende la comunicazione di informazioni in modo consono all'età dei minori interessati.

3. Le norme sul diritto all'informazione contenute nelle norme dell'Unione applicabili in materia di protezione dei dati si applicano ai dati personali registrati nell'ECRIS-TCN e trattati ai fini del presente regolamento.

Articolo 48

Diritto di accesso ai dati personali, di rettifica e di cancellazione degli stessi conservati nel MID e limitazione del loro trattamento

1. Per esercitare i diritti di cui agli articoli da 15 a 18 del regolamento (UE) 2016/679, agli articoli da 17 a 20 del regolamento (UE) 2018/1725 e agli articoli 14, 15 e 16 della direttiva (UE) 2016/680, l'interessato ha il diritto di rivolgersi all'autorità competente di qualsiasi Stato membro, che esamina la richiesta e vi risponde.

2. Lo Stato membro che ha esaminato tale richiesta risponde senza indebito ritardo e in ogni caso entro 45 giorni dalla ricezione della richiesta. Tale termine può essere prorogato di 15 giorni, se necessario, tenuto conto della complessità e del numero delle richieste. Lo Stato membro che ha esaminato la richiesta informa l'interessato di tale proroga, e dei motivi del ritardo, entro 45 giorni dal ricevimento della richiesta. Gli Stati membri possono stabilire che tali risposte siano fornite da uffici centrali.

3. Qualora la richiesta di rettifica o cancellazione dei dati personali sia presentata a uno Stato membro diverso da quello competente per la verifica manuale delle identità diverse, lo Stato membro al quale è stata presentata contatta le autorità dello Stato membro competente per la verifica manuale delle identità diverse entro sette giorni. Lo Stato membro competente per la verifica manuale delle identità diverse verifica senza indebito ritardo, in ogni caso entro 30 giorni da tale contatto, l'esattezza dei dati e la liceità del loro trattamento Tale termine può essere prorogato di 15 giorni, se necessario, tenuto conto della complessità e del numero delle richieste. Lo Stato membro competente per la verifica manuale delle identità diverse informa lo Stato membro che l'ha contattato in merito a tale proroga unitamente ai motivi del ritardo. L'interessato è informato dallo Stato membro che ha contattato l'autorità dello Stato membro competente per la verifica manuale delle identità diverse in merito al prosieguo della procedura.

4. Qualora la richiesta di rettifica o cancellazione dei dati personali sia presentata a uno Stato membro in cui l'unità centrale ETIAS sia competente per la verifica manuale delle identità diverse, lo Stato membro al quale è stata presentata la richiesta contatta entro sette giorni l'unità centrale ETIAS per chiedere un suo parere. L'unità centrale ETIAS esprime il proprio parere senza indebito ritardo e in ogni caso entro 30 giorni dalla data in cui è stata contattata. Tale termine può essere prorogato di 15 giorni, se necessario, tenuto conto della complessità e del numero delle richieste. L'interessato è informato dallo Stato membro che ha contattato l'unità centrale ETIAS in merito al prosieguo della procedura.

5. Qualora da un esame emerga che i dati conservati nel MID sono inesatti o sono stati registrati illecitamente, lo Stato membro competente per la verifica manuale delle identità diverse o, ove non vi sia uno Stato membro competente per la verifica manuale delle identità diverse o qualora l'unità centrale ETIAS sia responsabile della verifica manuale delle identità diverse, lo Stato membro al quale è stata presentata la richiesta provvede a rettificare o cancellare tali dati senza indebito ritardo. L'interessato è informato per iscritto che i suoi dati sono stati rettificati o cancellati.

6. Qualora i dati conservati nel MID siano modificati da uno Stato membro durante il loro periodo di conservazione, tale Stato membro effettua il trattamento di cui all'articolo 27 e, se del caso, all'articolo 29 per determinare se i dati modificati debbano essere oggetto di un collegamento. Qualora dal trattamento non risulti alcuna corrispondenza, tale Stato membro cancella i dati dal fascicolo di conferma dell'identità. Qualora dal trattamento automatizzato risultino uno o più corrispondenze, tale Stato membro crea o aggiorna il relativo collegamento conformemente alle disposizioni pertinenti del presente regolamento.

7. Qualora non ritenga che i dati conservati nel MID siano inesatti o siano stati registrati illecitamente, lo Stato membro competente per la verifica manuale delle identità diverse o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta adotta una decisione amministrativa con la quale illustra per iscritto senza indugio all'interessato la ragione per cui non intende rettificare o cancellare i dati che lo riguardano.

8. La decisione di cui al paragrafo 7 fornisce all'interessato informazioni sulla possibilità di impugnare la decisione adottata sulla richiesta di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali e, se del caso, informazioni su come intentare un'azione o presentare un reclamo dinanzi alle autorità competenti o alle autorità giurisdizionali competenti e su qualunque tipo di assistenza, anche da parte delle autorità di controllo.

9. La richiesta di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali contiene le informazioni necessarie per identificare l'interessato. Tali informazioni sono utilizzate unicamente per consentire l'esercizio dei diritti di cui al presente articolo e sono cancellate subito dopo.

10. Lo Stato membro competente per la verifica manuale delle identità diverse o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta conserva una registrazione scritta della presentazione di una richiesta di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali e di come è stata trattata e mette senza indugio tale registrazione a disposizione delle autorità di controllo.

11. Il presente articolo lascia impregiudicate le limitazioni e le restrizioni riguardo ai diritti di cui al presente articolo ai sensi del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680.

Articolo 49

Portale web

1. È istituito un portale web allo scopo di facilitare l'esercizio del diritto di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali.

2. Il portale web contiene informazioni sui diritti e sulle procedure di cui agli articoli 47 e 48 e un'interfaccia utente che consente alle persone i cui dati sono trattati nel MID e che sono state informate della presenza di un collegamento rosso ai sensi dell'articolo 32, paragrafo 4, di ricevere le informazioni di contatto dell'autorità competente dello Stato membro competente per la verifica manuale delle identità diverse.

3. Per ottenere le informazioni di contatto dell'autorità competente dello Stato membro responsabile della verifica manuale delle identità diverse, la persona i cui dati sono trattati nel MID dovrebbe inserire il riferimento all'autorità responsabile della verifica manuale delle identità diverse di cui all'articolo 34, lettera d). Il portale web utilizza tale riferimento per estrarre le informazioni di contatto dell'autorità competente dello Stato membro responsabile della verifica manuale delle diverse identità. Il portale web comprende anche un modello di posta elettronica per facilitare la comunicazione tra l'utente del portale e l'autorità competente dello Stato membro responsabile della verifica manuale delle identità diverse. Tale indirizzo di posta elettronica include un campo per il numero di identificazione unico di cui all'articolo 34, lettera c), per consentire all'autorità competente dello Stato membro competente per la verifica manuale di identità diverse di identificare i dati in questione.

4. Gli Stati membri forniscono a eu-LISA i dettagli di contatto di tutte le autorità competenti a esaminare e rispondere alle richieste di cui agli articoli 47 e 48 e verificano periodicamente se tali dettagli di contatto sono aggiornati.

5. eu-LISA sviluppa il portale web e ne garantisce la gestione tecnica.

6. La Commissione adotta un atto delegato conformemente all'articolo 69 che stabilisce norme dettagliate sul funzionamento del portale web, compresa l'interfaccia utente, le lingue in cui il portale web è disponibile e il modello di posta elettronica.

Articolo 50

Comunicazione di dati personali a paesi terzi, organizzazioni internazionali e soggetti privati

Fatti salvi l'articolo 31 del regolamento (CE) n. 767/2008, gli articoli 25 e 26 del regolamento (UE) 2016/794, l'articolo 41 del regolamento (UE) 2017/2226, l'articolo 65 del regolamento (UE) 2018/1240 e la consultazione delle banche dati Interpol attraverso l'ESP in conformità dell'articolo 9, paragrafo 5, del presente regolamento, che sono conformi alle disposizioni del capo V del regolamento (UE) 2018/1725 e del capo V del regolamento (UE) 2016/679, i dati personali conservati nelle componenti dell'interoperabilità o da queste trattati o consultati non sono trasferiti o messi a disposizione di paesi terzi, organizzazioni internazionali o soggetti privati.

Articolo 51

Controllo delle autorità di controllo

1. Ciascuno Stato membro assicura che le autorità di controllo monitorino indipendentemente la legittimità del trattamento dei dati personali ai sensi del presente regolamento da parte dello Stato membro interessato, compresa la loro trasmissione alle componenti dell'interoperabilità e viceversa.

2. Ciascuno Stato membro provvede affinché le disposizioni legislative, regolamentari e amministrative nazionali adottate ai sensi della direttiva (UE) 2016/680 siano altresì applicabili, ove necessario, in merito all'accesso alle componenti dell'interoperabilità da parte delle autorità di polizia e delle autorità designate, anche per quanto riguarda i diritti delle persone i cui dati sono così consultati.

3. Le autorità di controllo provvedono affinché, almeno ogni quattro anni, sia svolto un audit dei trattamenti di dati personali da parte delle autorità nazionali competenti ai fini del presente regolamento conformemente ai pertinenti principi internazionali di audit.

Le autorità di controllo pubblicano ogni anno il numero delle richieste di rettifica, cancellazione o limitazione del trattamento dei dati personali, le conseguenti azioni intraprese e il numero delle rettifiche, cancellazioni e limitazioni del trattamento effettuate in seguito alle richieste degli interessati.

4. Gli Stati membri provvedono affinché le proprie autorità di controllo dispongano delle risorse e delle competenze sufficienti per assolvere i compiti loro assegnati dal presente regolamento.

5. Gli Stati membri comunicano qualsiasi informazione richiesta da un'autorità di controllo di cui all'articolo 51, paragrafo 1, del regolamento (UE) 2016/679 e, in particolare, le forniscono informazioni sulle attività svolte conformemente alle loro responsabilità ai sensi del presente regolamento. Gli Stati membri consentono alle autorità di controllo di cui all'articolo 51, paragrafo 1, del regolamento (UE) 2016/679 di accedere alle loro registrazioni di cui agli articoli 10, 16, 24 e 36 del presente regolamento, di accedere alle loro giustificazioni di cui all'articolo 22, paragrafo 2, del presente regolamento, e di accedere in qualsiasi momento a tutti i loro locali utilizzati ai fini dell'interoperabilità.

Articolo 52

Audit del garante europeo della protezione dei dati

Il garante europeo della protezione dei dati provvede affinché almeno ogni quattro anni sia svolto un audit delle operazioni di trattamento dei dati personali effettuate da eu-LISA, dall'unità centrale ETIAS e da Europol ai fini del presente regolamento conformemente ai pertinenti principi internazionali di audit. Una relazione su tale audit è trasmessa al Parlamento europeo, al Consiglio, a eu-LISA, alla Commissione, agli Stati membri e all'agenzia dell'Unione interessata. A eu-LISA, all'unità centrale ETIAS e a Europol è data la possibilità di presentare osservazioni prima dell'adozione della relazione.

eu-LISA e l'unità centrale ETIAS ed Europol forniscono al garante europeo della protezione dei dati le informazioni da questo richieste, consentono al garante europeo della protezione dei dati di accedere a tutti i documenti che richiede e alle loro registrazioni di cui agli articoli 10, 16, 24 e 36 e gli consentono di accedere in qualsiasi momento a tutti i loro locali.

Articolo 53

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 nell'ambito delle rispettive responsabilità e assicurano il controllo coordinato dell'uso delle componenti dell'interoperabilità e dell'applicazione delle altre disposizioni del presente regolamento, in particolare se il garante europeo della protezione dei dati o un'autorità nazionale di controllo constata notevoli differenze tra le pratiche degli Stati membri o trasferimenti potenzialmente illeciti nell'uso dei canali di comunicazione delle componenti dell'interoperabilità.

2. Nei casi di cui al paragrafo 1 del presente articolo, è assicurato il controllo coordinato a norma dell'articolo 62 del regolamento (UE) 2018/1725.

3. Entro il 12 giugno 2021 e, successivamente, ogni due anni, il comitato europeo per la protezione dei dati trasmette al Parlamento europeo, al Consiglio, alla Commissione, a Europol, all'Agenzia europea della guardia di frontiera e costiera e a eu-LISA una relazione congiunta sulle sue attività ai sensi del presente articolo. Tale relazione comprende un capitolo su ciascuno Stato membro redatto dall'autorità di controllo dello Stato membro interessato.

CAPO VIII

Responsabilità

Articolo 54

Responsabilità di eu-LISA in fase di progettazione e sviluppo

1. eu-LISA garantisce che le infrastrutture centrali delle componenti dell'interoperabilità siano gestite conformemente al presente regolamento.

2. Le componenti dell'interoperabilità sono ospitate da eu-LISA nei suoi siti tecnici e forniscono le funzionalità di cui al presente regolamento nel rispetto delle condizioni di sicurezza, disponibilità, qualità e prestazione di cui all'articolo 55, paragrafo 1.

3. eu-LISA è responsabile dello sviluppo delle componenti dell'interoperabilità e di ogni adattamento necessario per istituire l'interoperabilità tra i sistemi centrali dell'EES, del VIS, dell'ETIAS, del SIS, dell'Eurodac e dell'ECRIS-TCN e l'ESP, il BMS comune, il CIR, il MID e il CRRS.

Fatto salvo l'articolo 62, eu-LISA non ha accesso a nessuno dei dati personali trattati attraverso l'ESP, il BMS comune, il CIR o il MID.

eu-LISA definisce la progettazione dell'architettura fisica delle componenti dell'interoperabilità, comprese le rispettive infrastrutture di comunicazione, e le specifiche tecniche e la loro evoluzione per quanto riguarda l'infrastruttura centrale e l'infrastruttura di comunicazione sicura, che sono adottate dal consiglio di amministrazione previo parere favorevole della Commissione. eu-LISA provvede anche agli adattamenti del SIS, dell'Eurodac o dell'ECRIS-TCN resi necessari dall'interoperabilità e previsti dal presente regolamento.

eu-LISA sviluppa e implementa le componenti dell'interoperabilità non appena possibile dopo l'entrata in vigore del presente regolamento e l'adozione da parte della Commissione delle misure di cui all'articolo 8, paragrafo 2, all'articolo 9, paragrafo 7, all'articolo 28, paragrafi 5 e 7, all'articolo 37, paragrafo 4, all'articolo 38, paragrafo 3, all'articolo 39, paragrafo 5, all'articolo 43, paragrafo 5, e all'articolo 74, paragrafo 10.

Lo sviluppo comporta l'elaborazione e l'applicazione delle specifiche tecniche, il collaudo e la gestione e il coordinamento generale del progetto.

4. In fase di progettazione e di sviluppo, è istituito un consiglio di gestione del programma composto di un massimo di 10 membri. Esso è costituito da sette membri nominati dal consiglio di amministrazione di eu-LISA tra i suoi membri o i supplenti, dal presidente del gruppo consultivo sull'interoperabilità di cui all'articolo 71, da un membro che rappresenta eu-LISA nominato dal suo direttore esecutivo e da un membro nominato dalla Commissione. I membri nominati dal consiglio di amministrazione di eu-LISA sono eletti soltanto tra detti Stati membri che sono pienamente vincolati, in base al diritto dell'Unione, dagli strumenti giuridici che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi di informazione dell'UE e che partecipano alle componenti dell'interoperabilità.

5. Il consiglio di gestione del programma si riunisce periodicamente, almeno tre volte a trimestre. Esso garantisce l'adeguata gestione della fase di progettazione e sviluppo delle componenti dell'interoperabilità.

Il consiglio di gestione del programma presenta mensilmente relazioni scritte al consiglio di amministrazione di eu-LISA sui progressi del progetto. Il consiglio di gestione del programma non ha potere decisionale, né mandato di rappresentare i membri del consiglio di amministrazione di eu-LISA.

6. Il consiglio di amministrazione di eu-LISA stabilisce il regolamento interno del consiglio di gestione del programma, che comprende in particolare disposizioni concernenti:

a) la presidenza;

b) i luoghi di riunione;

c) la preparazione delle riunioni;

d) l'ammissione di esperti alle riunioni;

e) i piani di comunicazione atti a garantire che i membri non partecipanti del consiglio di amministrazione siano tenuti pienamente informati.

La presidenza è esercitata da uno Stato membro che è pienamente vincolato, in base al diritto dell'Unione, dagli strumenti giuridici che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi di informazione dell'UE e che parteciperà ai componenti dell'interoperabilità.

Tutte le spese di viaggio e di soggiorno sostenute dai membri del consiglio di gestione del programma sono a carico di eu-LISA e l'articolo 10 del suo regolamento interno si applica mutatis mutandis. eu-LISA fornisce un segretariato al consiglio di gestione del programma.

Il gruppo consultivo sull'interoperabilità di cui all'articolo 71 si riunisce regolarmente fino all'entrata in funzione delle componenti dell'interoperabilità. Dopo ciascuna riunione, riferisce al consiglio di gestione del programma. Fornisce la consulenza tecnica a sostegno delle attività del consiglio di gestione del programma e monitora lo stato di preparazione degli Stati membri.

Articolo 55

Responsabilità di eu-LISA in seguito all'entrata in funzione

1. In seguito all'entrata in funzione di ciascuna componente dell'interoperabilità, eu-LISA è responsabile della gestione tecnica dell'infrastruttura centrale delle componenti dell'interoperabilità, compresi la manutenzione e gli sviluppi tecnologici. In cooperazione con gli Stati membri, provvede a che siano utilizzate, previa analisi costi/benefici, le migliori tecnologie disponibili. eu-LISA è inoltre responsabile della gestione tecnica dell'infrastruttura di comunicazione di cui agli articoli 6, 12, 17, 25 e 39.

La gestione tecnica delle componenti dell'interoperabilità consiste nell'insieme dei compiti e delle soluzioni tecniche necessari per garantire il funzionamento delle componenti dell'interoperabilità e fornendo ininterrottamente servizi agli Stati membri e alle agenzie dell'Unione 24 ore su 24 e 7 giorni su 7 in conformità del presente regolamento. Essa comprende la manutenzione e gli adeguamenti tecnici necessari per garantire che le componenti funzionino a un livello di qualità tecnica soddisfacente, specialmente per quanto riguarda i tempi di risposta alle interrogazioni dell'infrastruttura centrale, conformemente alle specifiche tecniche.

Tutte le componenti dell'interoperabilità sono sviluppate e gestite in modo tale da garantire una disponibilità rapida, continuata, efficiente e un accesso controllato, pieno e ininterrotto delle componenti e dei dati conservati nel MID, nel BMS comune e nel CIR, e un tempo di risposta in linea con le esigenze operative delle autorità degli Stati membri e delle agenzie dell'Unione.

2. Fatto salvo l'articolo 17 dello statuto dei funzionari dell'Unione europea, eu-LISA applica a tutti i membri del proprio personale che operano con i dati conservati nelle componenti dell'interoperabilità adeguate norme in materia di segreto professionale o altri obblighi di riservatezza equivalenti. Tale obbligo vincola il personale anche dopo che ha lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

Fatto salvo l'articolo 62, eu-LISA non ha accesso a nessuno dei dati personali trattati attraverso l'ESP, il BMS comune, il CIR e il MID.

3. eu-LISA sviluppa e mantiene un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati conservati nel BMS comune e nel CIR conformemente all'articolo 37.

4. eu-LISA svolge compiti relativi alla formazione sull'uso tecnico delle componenti dell'interoperabilità.

Articolo 56

Responsabilità degli Stati membri

1. Ciascuno Stato membro è responsabile di quanto segue:

a) la connessione all'infrastruttura di comunicazione dell'ESP e del CIR;

b) l'integrazione dei sistemi e delle infrastrutture nazionali esistenti con l'ESP, il CIR e il MID;

c) l'organizzazione, la gestione, il funzionamento e la manutenzione della propria infrastruttura nazionale esistente e della sua connessione alle componenti dell'interoperabilità;

d) la gestione e le modalità di accesso all'ESP, al CIR e al MID del personale debitamente autorizzato delle autorità nazionali competenti, quale che sia il tipo di autorizzazione, a norma del presente regolamento, nonché la creazione e l'aggiornamento periodico di un elenco di tale personale con le relative qualifiche;

e) l'adozione delle misure legislative di cui all'articolo 20, paragrafo 5, e paragrafo 6, ai fini dell'accesso al CIR a fini di identificazione;

f) la verifica manuale delle identità diverse di cui all'articolo 29;

g) la conformità ai requisiti di qualità dei dati stabiliti dal diritto dell'Unione;

h) la conformità alle norme di ciascun sistema di informazione dell'UE riguardanti la sicurezza e l'integrità dei dati personali;

i) la correzione delle carenze riscontrate nella relazione di valutazione della Commissione riguardante la qualità dei dati di cui all'articolo 37, paragrafo 5.

2. Ciascuno Stato membro provvede alla connessione delle rispettive autorità designate al CIR.

Articolo 57

Responsabilità di Europol

1. Europol provvede al trattamento delle interrogazioni dei dati Europol effettuate tramite l'ESP e adatta di conseguenza la sua interfaccia QUEST («Querying Europol Systems») per i dati con un livello di protezione minimo.

2. Europol è responsabile della gestione e delle modalità d'uso e di accesso all'ESP e all'archivio comune di dati di identità da parte del suo personale debitamente autorizzato, a norma del presente regolamento, nonché della creazione e dell'aggiornamento periodico di un elenco di tale personale con le relative qualifiche.

Articolo 58

Responsabilità dell'unità centrale ETIAS

L'unità centrale ETIAS è responsabile di quanto segue:

a) la verifica manuale delle identità diverse a norma dell'articolo 29;

b) la rilevazione di identità multiple tra i dati conservati nell'EES, nel VIS, nell'Eurodac e nel SIS di cui all'articolo 65.

CAPO IX

Modifiche di altri strumenti dell'Unione

Articolo 59

Modifiche del regolamento (UE) 2018/1726

Il regolamento (UE) 2018/1726 è così modificato:

1) l'articolo 12 è sostituito dal seguente:

«*Articolo 12*

Qualità dei dati

1. Fatte salve le responsabilità degli Stati membri per quanto riguarda i dati inseriti nei sistemi sotto la responsabilità operativa dell'Agenzia, quest'ultima, in stretta collaborazione con i suoi gruppi consultivi, predispone, per tutti i sistemi di cui ha la responsabilità operativa, procedure e meccanismi automatizzati di controllo della qualità dei dati, indicatori comuni della qualità dei dati e norme minime di qualità per conservare i dati, in conformità degli strumenti giuridici che disciplinano tali sistemi di informazione e dell'articolo 37 dei regolamenti (UE) 2019/817 (*) e (UE) 2019/818 (**) del Parlamento europeo e del Consiglio.

2. L'Agenzia istituisce un archivio centrale, contenente unicamente dati anonimizzati, di relazioni e statistiche a norma dell'articolo 39 dei regolamenti (UE) 2019/817 e (UE) 2019/818, fatte salve specifiche disposizioni contenute negli strumenti giuridici che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi IT su larga scala gestiti dall'Agenzia.

(*) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).

(**) Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità dei sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, dell'asilo e della migrazione e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85).»;

2) all'articolo 19, il paragrafo 1 è così modificato:

a) è inserita la lettera seguente:

«ee *bis*) adotta relazioni sulla situazione dello sviluppo delle componenti dell'interoperabilità a norma dell'articolo 78, paragrafo 2, del regolamento (UE) 2019/817 e dell'articolo 74, paragrafo 2, del regolamento (UE) 2019/818;»;

b) la lettera ff) è sostituita dalla seguente:

«ff) adotta relazioni sul funzionamento tecnico del SIS II in conformità dell'articolo 60, paragrafo 7, del regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio (*) e dell'articolo 74, paragrafo 8, del regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio (**), sul funzionamento tecnico del VIS in conformità dell'articolo 50, paragrafo 3, del regolamento (CE) n. 767/2008 e dell'articolo 17, paragrafo 3, della decisione 2008/633/GAI, dell'EES in conformità dell'articolo 72, paragrafo 4, del regolamento (UE) 2017/2226, dell'ETIAS in conformità dell'articolo 92, paragrafo 4, del regolamento (UE) 2018/1240, dell'ECRIS-TCN e dell'implementazione di riferimento ECRIS in conformità dell'articolo 36, paragrafo 8, del regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio (***) e sul funzionamento delle componenti dell'interoperabilità in conformità dell'articolo 78, paragrafo 3, del regolamento (UE) 2019/817 e dell'articolo 74, paragrafo 3, del regolamento (UE) 2019/818»;

(*) Regolamento (UE) 2018/1861 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 (GU L 312 del 7.12.2018, pag. 14).

(**) Regolamento (UE) 2018/1862 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 della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312, del 7.12.2018, pag. 56).

(***) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1).»;

c) la lettera hh) è sostituita dalla seguente:

«hh) adotta osservazioni formali sulle relazioni del Garante europeo della protezione dei dati relative ai suoi controlli in conformità dell'articolo 56, paragrafo 2, del regolamento (UE) 2018/1861, dell'articolo 42, paragrafo 2, del regolamento (CE) n. 767/2008, dell'articolo 31, paragrafo 2, del regolamento (UE) n. 603/2013, dell'articolo 56, paragrafo 2, del regolamento (UE) 2017/2226, dell'articolo 67 del regolamento (UE) 2018/1240, dell'articolo 29, paragrafo 2, del regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio e dell'articolo 52 dei regolamenti (UE) 2019/817 e (UE) 2019/818 e assicura adeguato seguito a tali controlli;»;

d) la lettera mm) è sostituita dalla seguente:

«mm) provvede alla pubblicazione annuale dell'elenco delle autorità competenti autorizzate a consultare direttamente i dati inseriti nel SIS II in conformità dell'articolo 41, paragrafo 8, del regolamento (UE) 2018/1861 e dell'articolo 56, paragrafo 7, del regolamento (UE) 2018/1862, nonché dell'elenco degli uffici dei sistemi nazionali del SIS II (N.SIS) e degli uffici SIRENE di cui, rispettivamente, all'articolo 7, paragrafo 3, del regolamento (UE) 2018/1861 e all'articolo 7, paragrafo 3, del regolamento (UE) 2018/1862, come pure dell'elenco delle autorità competenti di cui all'articolo 65, paragrafo 2, del regolamento (UE) 2017/2226, dell'elenco delle autorità competenti di cui all'articolo 87, paragrafo 2, del regolamento (UE) 2018/1240, dell'elenco delle autorità centrali di cui all'articolo 34, paragrafo 2, del regolamento (UE) 2019/816 e dell'elenco delle autorità di cui all'articolo 71, paragrafo 1, del regolamento (UE) 2019/817 e all'articolo 67, paragrafo 1, del regolamento (UE) 2019/818.»;

3) all'articolo 22, il paragrafo 4 è sostituito dal seguente:

«4. Europol e Eurojust possono assistere alle riunioni del consiglio di amministrazione in qualità di osservatori quando sono all'ordine del giorno questioni concernenti il SIS II, in relazione all'applicazione della decisione 2007/533/GAI.

L'Agenzia europea della guardia di frontiera e costiera può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore quando sono all'ordine del giorno questioni concernenti il SIS, in relazione all'applicazione del regolamento (UE) 2016/1624.

Europol può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore quando sono all'ordine del giorno questioni concernenti il VIS, in relazione all'applicazione della decisione 2008/633/GAI, o questioni concernenti l'Eurodac, in relazione all'applicazione del regolamento (UE) n. 603/2013.

Europol può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore quando sono all'ordine del giorno questioni concernenti l'EES, in relazione all'applicazione del regolamento (UE) 2017/2226, o questioni concernenti l'ETIAS, in relazione al regolamento (UE) 2018/1240.

L'Agenzia europea della guardia di frontiera e costiera può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore anche quando è all'ordine del giorno una questione concernente l'ETIAS in relazione all'applicazione del regolamento (UE) 2018/1240.

Europol, Eurojust e la Procura europea possono assistere alle riunioni del consiglio di amministrazione in qualità di osservatori quando è all'ordine del giorno una questione concernente il regolamento (UE) 2019/816.

Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera possono assistere alle riunioni del consiglio di amministrazione in qualità di osservatori quando è all'ordine del giorno una questione concernente il regolamento (UE) 2019/817 e (UE) 2019/818.

Il consiglio di amministrazione può invitare qualsiasi altra persona, il cui parere possa essere rilevante, a presenziare alle riunioni in veste di osservatore.»;

4) all'articolo 24, paragrafo 3, la lettera p) è sostituita dalla seguente:

«p) fatto salvo l'articolo 17 dello statuto dei funzionari, stabilire le clausole di riservatezza per conformarsi all'articolo 17 del regolamento (CE) n. 1987/2006, all'articolo 17 della decisione 2007/533/GAI, all'articolo 26, paragrafo 9, del regolamento (CE) n. 767/2008, all'articolo 4, paragrafo 4, del regolamento (UE) n. 603/2013, all'articolo 37, paragrafo 4, del regolamento (UE) 2017/2226, all'articolo 74, paragrafo 2, del regolamento (UE) 2018/1240, all'articolo 11, paragrafo 16, del regolamento (UE) 2019/816 e all'articolo 55, paragrafo 2, dei regolamenti (UE) 2019/817 e (UE) 2019/818;»;

5) l'articolo 27 è così modificato:

a) al paragrafo 1, è inserita la lettera seguente:

«d *bis*) gruppo consultivo sull'interoperabilità;»;

b) il paragrafo 3 è sostituito dal seguente:

«3. Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera possono nominare un rappresentante ciascuno in seno al gruppo consultivo SIS II.

Europol può nominare un rappresentante in seno ai gruppi consultivi VIS ed Eurodac ed EES-ETIAS.

L'Agenzia europea della guardia di frontiera e costiera può nominare anche un rappresentante in seno al gruppo consultivo EES-ETIAS.

Eurojust, Europol olamento si applica al trattamento delle informazioni sull'identità dei cittadini di paesi terzi che sono stati oggetto di condanne negli Stati meCRIS-TCN.

Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera possono nominare un rappresentante ciascuno in seno al gruppo consultivo sull'interoperabilità.».

Articolo 60

Modifiche del regolamento (UE) n. 2018/1862

Il regolamento (UE) 2018/1862 è così modificato:

1) all'articolo 3 sono aggiunti i seguenti punti:

«18) "ESP": il portale di ricerca europeo quale istituito dall'articolo 6, paragrafo 1, del regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio (*);

19) "BMS comune": il servizio comune di confronto biometrico quale istituito dall'articolo 12, paragrafo 1, del regolamento (UE) 2019/818;

20) "CIR": l'archivio comune di dati di identità quale istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/818;

21) "MID": il rilevatore di identità multiple quale istituito dall'articolo 25, paragrafo 1, del regolamento (UE) 2019/818.

(*) Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2018, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85)»;

2) l'articolo 4 è così modificato:

a) al paragrafo 1 le lettere sono sostituite dalle seguenti:

«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;

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 dati tra gli uffici SIRENE di cui all'articolo 7, paragrafo 2; e

d) un'infrastruttura di comunicazione sicura tra il CS-SIS e le infrastrutture centrali dell'ESP, del BMS comune e del MID. »;

b) sono aggiunti i paragrafi seguenti:

«8. Fatti salvi i paragrafi da 1 a 5, i dati SIS sulle persone e sui documenti di identità possono essere consultati tramite l'ESP.

9. Fatti salvi i paragrafi da 1 a 5, i dati SIS sulle persone e sui documenti di identità possono essere trasmessi tramite l'infrastruttura di comunicazione sicura prevista al paragrafo 1, lettera d). La trasmissione è limitata alla misura in cui i dati siano necessari ai fini del regolamento (UE) 2019/818.»;

3) all'articolo 7 è inserito il paragrafo seguente:

«2 *bis*. Gli uffici SIRENE provvedono alla verifica manuale delle identità diverse a norma dell'articolo 29 del regolamento (UE) 2019/818. Nella misura necessaria ad assolvere tale compito, gli uffici SIRENE hanno accesso ai dati conservati nel CIR e nel MID per le finalità previste agli articoli 21 e 26 del regolamento (UE) 2019/818.»;

4) all'articolo 12, paragrafo 1, è aggiunto il comma seguente:

«Gli Stati membri provvedono affinché ogni accesso ai dati personali tramite l'ESP sia registrato per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati e ai fini dell'autocontrollo e dell'integrità e sicurezza ei dati.»;

5) all'articolo 44, paragrafo 1, è aggiunta la lettera seguente:

«f) della verifica delle identità diverse e del contrasto della frode di identità in conformità del capo V del regolamento (UE) 2019/818.»;

6) all'articolo 74, il paragrafo 7 è sostituito dal seguente:

«7. Ai fini dell'articolo 15, paragrafo 4, e dei paragrafi 3, 4 e 6 del presente articolo, eu-LISA memorizza nell'archivio centrale per le relazioni e statistiche di cui all'articolo 39 del regolamento (UE) 2019/818 i dati di cui dell'articolo 15, paragrafo 4, e al paragrafo 3 del presente articolo, che non consentono l'identificazione delle persone fisiche.

eu-LISA permette alla Commissione e agli organismi di cui al paragrafo 6 del presente articolo di ottenere relazioni e statistiche personalizzate. Su richiesta, eu-LISA concede agli Stati membri, alla Commissione, a Europol e all'Agenzia europea della guardia di frontiera e costiera l'accesso all'archivio centrale per le relazioni e le statistiche in conformità dell'articolo 39 del regolamento (UE) 2019/818.».

Articolo 61

Modifiche del regolamento (UE) 2019/816

Il regolamento (UE) 2019/816 è così modificato:

1) all'articolo 1 è aggiunta la lettera seguente:

«c) le condizioni alle quali l'ECRIS-TCN concorre ad agevolare e contribuire alla corretta identificazione delle persone registrate nell'ECRIS-TCN conformemente alle condizioni e ai fini di cui all'articolo 20 del regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio (*), conservando nel CIR i dati di identità, i dati del documento di viaggio e i dati biometrici.

(*) Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85)»;

2) l'articolo 2 è sostituito dal seguente:

«*Articolo 2*

Ambito di applicazione

Il presente regolamento si applica al trattamento delle informazioni sull'identità dei cittadini di paesi terzi che sono stati oggetto di condanne negli Stati membri, allo scopo di individuare gli Stati membri in cui sono state pronunciate tali condanne. Ad eccezione dell'articolo 5, paragrafo 1, lettera b), punto ii), le disposizioni del presente regolamento che si applicano ai cittadini di paesi terzi si applicano anche ai cittadini dell'Unione che hanno anche la cittadinanza di un paese terzo e che sono stati oggetto di condanne negli Stati membri. Il presente regolamento inoltre agevola e aiuta nella corretta identificazione delle persone, in conformità del presente regolamento e del regolamento (UE) 2019/818.»;

3) l'articolo 3 è così modificato:

a) il punto 8) è soppresso;

b) sono aggiunti i punti seguenti:

«19) "CIR", l'archivio comune di dati di identità quale istituito dall'articolo 17, paragrafo 1, del regolamento (UE) 2019/818;

20) "dati dell'ECRIS-TCN", tutti i dati conservati nel sistema centrale dell'ECRIS-TCN e nel CIR conformemente all'articolo 5;

21) "ESP", il portale di ricerca europeo istituito dall'articolo 6, paragrafo 1, del regolamento (UE) 2019/818.»;

4) all'articolo 4, il paragrafo 1 è così modificato:

a) la lettera a) è sostituita dalla seguente:

«a) un sistema centrale;»;

b) è inserita la lettera seguente:

«a *bis*) il CIR;»;

c) è aggiunta la lettera seguente:

«e) un'infrastruttura di comunicazione tra il sistema centrale e le infrastrutture centrali dell'ESP e del CIR;»;

5) l'articolo 5 è così modificato:

a) al paragrafo 1, la parte introduttiva è sostituita dalla seguente:

«1. Per ciascun cittadino condannato di un paese terzo, l'autorità centrale dello Stato membro di condanna crea un registro dei dati in ECRIS-TCN. La registrazione dei dati comprende:»;

b) è inserito il paragrafo seguente:

«1 *bis*. Il CIR contiene i dati di cui al paragrafo 1, lettera b), e i seguenti dati di cui al paragrafo 1, lettera a): cognome; nome o nomi; data di nascita; luogo di nascita (città e paese); la o le cittadinanze; sesso; se del caso, nomi precedenti e, ove disponibili, pseudonimi, come pure, ove disponibili, tipo e numero del documento o dei documenti di viaggio dell'interessato, nonché denominazione dell'autorità di rilascio. Il CIR può inoltre contenere i dati di cui al paragrafo 3. I rimanenti dati dell'ECRIS-TCN sono conservati nel sistema centrale.»;

6) l'articolo 8 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. Ciascuna registrazione di dati è conservata nel sistema centrale e nel CIR fintanto che i dati relativi alla condanna o alle condanne pronunciate a carico dell'interessato sono conservati nel casellario giudiziale.»;

b) il paragrafo 2 è sostituito dal seguente:

«2. Allo scadere del periodo di conservazione di cui al paragrafo 1, l'autorità centrale dello Stato membro di condanna cancella dal sistema centrale e dal CIR la registrazione di dati, inclusi i dati relativi alle impronte digitali o le immagini del volto. Tale cancellazione avviene automaticamente, se possibile, e in ogni caso non oltre un mese dalla scadenza del periodo di conservazione.»;

7) l'articolo è così modificato:

a) al paragrafo 1, i termini «ECRIS-TCN» sono sostituiti, con gli opportuni adattamenti grammaticali, da «sistema centrale e CIR»;

b) ai paragrafi 2, 3 e 4, i termini «sistema centrale» sono sostituiti, con gli opportuni adattamenti grammaticali, da «sistema centrale e CIR»;

8) all'articolo 10, paragrafo 1, la lettera j) è soppressa;

9) all'articolo 12, paragrafo 2, i termini «sistema centrale» sono sostituiti, con gli opportuni adattamenti grammaticali, da «sistema centrale dell'ECRIS-TCN e CIR».

10) all'articolo 13, paragrafo 2, i termini «sistema centrale» sono sostituiti, con gli opportuni adattamenti grammaticali, da «sistema centrale, CIR».

11) all'articolo 23, paragrafo 2, i termini «sistema centrale» sono sostituiti, con gli opportuni adattamenti grammaticali, da «sistema centrale e CIR»;

12) l'articolo 24 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

«1. I dati inseriti nel sistema centrale e nel CIR sono trattati ai soli fini di individuare lo Stato membro o gli Stati membri in possesso di informazioni sui precedenti penali di cittadini di paesi terzi. I dati inseriti nel CIR sono inoltre trattati in conformità del regolamento (UE) 2019/818 al fine di agevolare e contribuire alla corretta identificazione delle persone registrate nel sistema ECRIS-TCN in conformità del presente regolamento.»;

b) è aggiunto il paragrafo seguente:

«3. Fatto salvo il paragrafo 2, l'accesso ai fini della consultazione dei dati conservati nel CIR è riservato altresì al personale debitamente autorizzato delle autorità nazionali di ciascuno Stato membro e al personale debitamente autorizzato delle agenzie dell'Unione che sono competenti per gli scopi di cui agli articoli 20 e 21 del regolamento (UE) 2019/818. Tale accesso è limitato conformemente alla misura in cui i dati siano necessari all'assolvimento dei propri compiti per tali scopi, ed è proporzionato agli obiettivi perseguiti.»;

13) all'articolo 32, il paragrafo 2 è sostituito dal seguente:

«2. Ai fini del paragrafo 1, eu-LISA conserva i dati di cui a tale paragrafo nell'archivio centrale per le relazioni e le statistiche di cui all'articolo 39 del regolamento (UE) 2019/818.»;

14) all'articolo 33, paragrafo 1, i termini «sistema centrale» sono sostituiti, con gli opportuni adattamenti grammaticali, da «sistema centrale, CIR e ».

15) all'articolo 41, il paragrafo 2 è sostituito dal seguente:

«2. Per le condanne pronunciate prima della data dell'avvio dell'inserimento dei dati ai sensi dell'articolo 35, paragrafo 1, le autorità centrali creano la registrazione di dati individuale nel sistema centrale e nel CIR come segue:

a) i dati alfanumerici che devono essere inseriti nel sistema centrale e nel CIR entro la fine del periodo di cui all'articolo 35, paragrafo 2;

b) i dati relativi alle impronte digitali che devono essere inseriti nel CIR entro due anni dall'entrata in funzione ai sensi dell'articolo 35, paragrafo 4.».

CAPO X

Disposizioni finali

Articolo 62

Comunicazione e valutazione

1. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione, unicamente per elaborare relazioni e statistiche, del numero di interrogazioni per utente del profilo ESP.

Non è possibile l'identificazione individuale dai dati.

2. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi al CIR, unicamente per elaborare relazioni e statistiche:

a) numero di interrogazioni ai fini degli articoli 20, 21 e 22;

b) cittadinanza, genere e anno di nascita della persona interessata;

c) tipo del documento di viaggio e codice a tre lettere del paese di rilascio;

d) numero di interrogazioni effettuate con dati biometrici e senza.

Non è possibile l'identificazione individuale dai dati.

3. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi al MID, unicamente per elaborare relazioni e statistiche:

a) numero di interrogazioni effettuate con dati biometrici e senza;

b) numero di ciascun tipo di collegamento e i sistemi di informazione dell'UE contenenti i dati di collegamento;

c) periodo di tempo in cui un collegamento giallo e rosso è rimasto nel sistema.

Non è possibile l'identificazione individuale dai dati.

4. Il personale debitamente autorizzato dell'Agenzia europea della guardia di frontiera e costiera ha accesso alla consultazione dei dati di cui ai paragrafi 1, 2 e 3 del presente articolo ai fini dell'esecuzione delle analisi del rischio e delle valutazioni delle vulnerabilità di cui agli articoli 11 e 13 del regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio ([38]).

5. Il personale debitamente autorizzato di Europol ha accesso alla consultazione dei dati di cui ai paragrafi 2 e 3 del presente articolo ai fini dell'esecuzione delle analisi strategiche, tematiche e operative di cui all'articolo 18, paragrafo 2, lettere b) e c), del regolamento (UE) 2016/794.

6. Ai fini dei paragrafi l, 2 e 3, eu-LISA conserva i dati di cui a tali paragrafi nel CRRS. Non è possibile l'identificazione individuale dai dati figuranti nel CRRS, ma i dati permettono alle autorità di cui ai paragrafi l, 2 e 3 di ricavare relazioni e dati statistici personalizzabili al fine di migliorare l'efficienza delle verifiche di frontiera, assistere le autorità nel trattamento delle domande di visto e sostenere politiche migratorie dell'Unione basate su dati concreti.

7. Su richiesta, la Commissione mette a disposizione dell'Agenzia dell'Unione europea per i diritti fondamentali le informazioni pertinenti al fine di valutare l'impatto del presente regolamento sui diritti fondamentali.

([38]) 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).

Articolo 63

Periodo transitorio per l'uso del portale di ricerca europeo

1. Per un periodo di due anni a partire dall'entrata in funzione dell'ESP gli obblighi di cui all'articolo 7, paragrafi 2 e 4, non si applicano e l'uso del portale è facoltativo.

2. Alla Commissione è conferito il potere di adottare un atto delegato conformemente all'articolo 69 al fine di modificare il presente regolamento prorogando una volta il termine di cui al paragrafo 1 del presente articolo di non oltre un anno, qualora una valutazione dell'attuazione dell'ESP abbia dimostrato che tale proroga è necessaria in particolare in vista dell'impatto dell'entrata in funzione dell'ESP sull'organizzazione e la lunghezza delle verifiche di frontiera.

Articolo 64

Periodo transitorio per l'applicazione delle disposizioni sull'accesso all'archivio comune di dati di identità a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi

L'articolo 22 si applica a partire dalla data di entrata in funzione del CIR di cui all'articolo 68, paragrafo 3.

Articolo 65

Periodo transitorio per il rilevatore di identità multiple

1. Per un periodo di un anno dopo che eu-LISA comunica il completamento del collaudo del MID di cui all'articolo 68, paragrafo 4, lettera b), e prima dell'entrata in funzione del MID, l'unità centrale ETIAS è competente per effettuare le rilevazioni di identità multiple tra i dati conservati nell'EES, nel VIS, nell'Eurodac e nel SIS. Le rilevazioni di identità multiple sono effettuate usando esclusivamente i dati biometrici.

2. Qualora dall'interrogazione risultino uno o più riscontri positivi e i dati di identità dei fascicoli oggetto del collegamento siano gli stessi o simili, è creato un collegamento bianco conformemente all'articolo 33.

Qualora dall'interrogazione risultino uno o più riscontri positivi e i dati di identità dei fascicoli oggetto del collegamento non possano essere considerati simili, è creato un collegamento giallo conformemente all'articolo 30 e si applica la procedura di cui all'articolo 29.

Qualora risultino più riscontri positivi è creato un collegamento tra tutti i dati per i quali è emerso un riscontro positivo.

3. Qualora sia creato un collegamento giallo il MID permette all'unità centrale ETIAS di consultare i dati di identità presenti nei vari sistemi di informazione dell'UE.

4. Qualora sia creato un collegamento con una segnalazione nel SIS diversa da una segnalazione creata ai sensi dell'articolo 3 del regolamento (UE) 2018/1860, degli articoli 24 e 25 del regolamento (UE) 2018/1861 o dell'articolo 38 del regolamento (UE) 2018/1862, il MID permette all'ufficio SIRENE dello Stato membro che ha creato la segnalazione di consultare i dati di identità presenti nei vari sistemi di informazione.

5. L'unità centrale ETIAS o, nei casi di cui al paragrafo 4 del presente articolo, l'ufficio SIRENE dello Stato membro che ha creato la segnalazione accede ai dati contenuti nel fascicolo di conferma dell'identità ed esamina le identità diverse, aggiorna il collegamento conformemente agli articoli 31, 32 e 33 e lo aggiunge al fascicolo di conferma dell'identità.

6. L'unità centrale ETIAS comunica alla Commissione le informazioni di cui all'articolo 67, paragrafo 3, solo dopo che tutti i collegamenti gialli siano stati verificati manualmente e i loro status aggiornati in collegamenti verdi, bianchi o rossi.

7. Se necessario gli Stati membri forniscono assistenza all'unità centrale ETIAS ai fini dello svolgimento delle rilevazioni di identità multiple a norma del presente articolo.

8. Alla Commissione è conferito il potere di adottare un atto delegato conformemente all'articolo 69 al fine di modificare il presente regolamento prorogando il termine di cui al paragrafo 1 del presente articolo di sei mesi, rinnovabile due volte per sei mesi alla volta. Tale proroga è concessa unicamente a seguito di una valutazione del tempo stimato per completare le rilevazioni di identità multiple di cui al presente articolo che dimostri che le rilevazioni di identità multiple non possono essere completate prima dello scadere del termine restante ai sensi del paragrafo 1 del presente articolo o di qualsiasi proroga in corso, per motivi indipendenti dall'unità centrale ETIAS e che non sia possibile applicare misure correttive. La valutazione è effettuata al più tardi tre mesi prima della scadenza di tale termine o della proroga in corso.

Articolo 66

Spese

1. Le spese sostenute per l'istituzione e il funzionamento dell'ESP, del BMS comune, del CIR e del MID sono a carico del bilancio dell'Unione.

2. Le spese sostenute per l'integrazione delle esistenti infrastrutture nazionali e la loro connessione alle interfacce nazionali uniformi nonché per ospitare le interfacce nazionali uniformi sono a carico del bilancio generale dell'Unione.

Sono escluse le seguenti spese:

a) l'ufficio di gestione di progetto degli Stati membri (riunioni, missioni, uffici);

b) l'hosting dei sistemi IT nazionali (spazio, implementazione, elettricità, impianti di raffreddamento);

c) la gestione di sistemi IT nazionali (operatori e contratti di assistenza);

d) la progettazione, lo sviluppo, l'implementazione, il funzionamento e la manutenzione di reti di comunicazione nazionali.

3. Fatti salvi gli ulteriori finanziamenti a tal fine da altre fonti del bilancio generale dell'Unione europea, un importo di 32 077 000 EUR è mobilitato dalla dotazione di 791 000 000 EUR prevista a norma dell'articolo 5, paragrafo 5, lettera b), del regolamento (UE) n. 515/2014 per coprire i costi di attuazione del presente regolamento, come previsto ai paragrafi 1 e 2 del presente articolo.

4. Dalla dotazione di cui al paragrafo 3, 22 861 000 EUR sono assegnati a eu-LISA, 9 072 000 EUR sono assegnati a Europol e 144 000 EUR sono assegnati all'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL), per sostenere tali agenzie nell'espletamento dei rispettivi compiti ai sensi del presente regolamento. Tali finanziamenti sono attuati in regime di gestione indiretta.

5. Le spese sostenute dalle autorità designate di cui all'articolo 4, punto 24), sono a carico di ciascuno Stato membro. Le spese per connettere al CIR ciascuna autorità designata sono a carico, rispettivamente, di ciascuno Stato membro.

Le spese sostenute da Europol, comprese quelle per connettersi al CIR, sono a carico di Europol.

Articolo 67

Comunicazioni

1. Gli Stati membri comunicano a eu-LISA i nominativi delle rispettive autorità di cui agli articoli 7, 20, 21 e 26 che possono usare l'ESP, il CIR e il MID o accedervi.

Entro tre mesi dall'entrata in funzione di ciascuna componente dell'interoperabilità a norma dell'articolo 68, un elenco consolidato di tali autorità è pubblicato nella Gazzetta ufficiale dell'Unione europea. Qualora l'elenco subisca modifiche, eu-LISA pubblica una volta all'anno un elenco consolidato aggiornato.

2. eu-LISA comunica alla Commissione il positivo completamento dei collaudi di cui all'articolo 68, paragrafo 1, lettera b), paragrafo 2, lettera b), paragrafo 3, lettera b), paragrafo 4, lettera b), paragrafo 5, lettera b) e paragrafo 6, lettera b).

3. L'unità centrale ETIAS comunica alla Commissione il positivo completamento del periodo transitorio di cui all'articolo 65.

4. La Commissione mette a disposizione degli Stati membri e del pubblico le informazioni comunicate a norma del paragrafo 1, tenendo costantemente aggiornata la pagina web.

Articolo 68

Entrata in funzione

1. La Commissione fissa la data a decorrere dalla quale l'ESP entra in funzione mediante un atto di esecuzione una volta che:

a) siano state adottate le misure di cui all'articolo 8, paragrafo 2, all'articolo 9, paragrafo 7, e all'articolo 443 paragrafo 5;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale dell'ESP che ha effettuato in cooperazione con le autorità degli Stati membri e le agenzie dell'Unione che potrebbero utilizzare l'ESP;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 8, paragrafo 1, e le abbia comunicate alla Commissione.

L'ESP consulta le banche dati Interpol solo se le disposizioni tecniche consentono di rispettare l'articolo 9, paragrafo 5. L'eventuale impossibilità di rispettare l'articolo 9, paragrafo 5, comporta la mancata consultazione delle banche dati Interpol da parte dell'ESP, ma non ritarda l'avvio delle attività dell'ESP.

La Commissione fissa la data di cui al primo comma, che dovrà cadere entro 30 giorni dall'adozione dell'atto di esecuzione.

2. La Commissione fissala data a decorrere dalla quale il BMS comune entra in funzione mediante un atto di esecuzione una volta che:

a) siano state adottate le misure di cui all'articolo 13, paragrafo 5 e all'articolo 43, paragrafo 5;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del BMS comune che deve essere effettuato in cooperazione con le autorità degli Stati membri;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 8, paragrafo 13, e le abbia comunicate alla Commissione;

d) eu-LISA abbia dichiarato il positivo completamento del collaudo di cui al paragrafo 5, lettera b).

La Commissione fissa la data di cui al primo comma, che dovrà cadere entro 30 giorni dall'adozione dell'atto di esecuzione.

3. La Commissione fissa la data a decorrere dalla quale il CIR entra in funzione mediante un atto di esecuzione una volta che:

a) siano state adottate le misure di cui all'articolo 43, paragrafo 5, e all'articolo 74, paragrafo 10;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del CIR che deve essere effettuato in cooperazione con le autorità degli Stati membri;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 18 e le abbia comunicate alla Commissione;

d) eu-LISA abbia dichiarato il positivo completamento del collaudo di cui al paragrafo 5, lettera b).

La Commissione fissa la data di cui al primo comma, che dovrà cadere entro 30 giorni dall'adozione dell'atto di esecuzione.

4. La Commissione fissa la data a decorrere dalla quale il MID entra in funzione mediante un atto di esecuzione una volta che:

a) siano state adottate le misure di cui all'articolo 28, paragrafi 5 e 7, all'articolo 32, paragrafo 5, all'articolo 33, paragrafo 6, all'articolo 43, paragrafo 5, e all'articolo 49, paragrafo 6;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del MID, che è effettuato in cooperazione con le autorità degli Stati membri e l'unità centrale ETIAS;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 34 e le abbia comunicate alla Commissione;

d) l'unità centrale ETIAS abbia comunicato alla Commissione le informazioni a norma dell'articolo 67, paragrafo 3;

e) eu-LISA abbia dichiarato il positivo completamento del collaudo di cui al paragrafo 1, lettera b), al paragrafo 2, lettera b), al paragrafo 3, lettera b), e al paragrafo 4, lettera b).

La Commissione fissa la data di cui al primo comma, che dovrà cadere entro 30 giorni dall'adozione degli atti di esecuzione.

5. La Commissione fissa la data a decorrere dalla quale i meccanismi e le procedure di controllo automatico della qualità dei dati, gli indicatori comuni per la qualità dei dati e le norme minime di qualità devono essere utilizzati mediante atti di esecuzione una volta che:

a) siano state adottate le misure di cui all'articolo 37, paragrafo 4;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale dei meccanismi e delle procedure di controllo automatico della qualità dei dati, degli indicatori comuni per la qualità dei dati e delle norme minime di qualità, che è effettuato in cooperazione con le autorità gli Stati membri.

La Commissione fissa la data di cui al primo comma, che dovrà cadere entro 30 giorni dall'adozione degli atti di esecuzione.

6. La Commissione fissa la data a decorrere dalla quale il CRRS entra in funzione mediante un atto di esecuzione una volta che:

a) siano state adottate le misure di cui all'articolo 39, paragrafo 5, e all'articolo 43, paragrafo 5;

b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale del CRRS che è effettuato in cooperazione con le autorità degli Stati membri;

c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 39 e le abbia comunicate alla Commissione.

La Commissione fissa la data di cui al primo comma, che dovrà cadere entro 30 giorni dall'adozione degli atti di esecuzione

7. La Commissione informa il Parlamento europeo e il Consiglio dell'esito dei collaudi effettuati a norma del paragrafo 1, lettera b), del paragrafo 2, lettera b), del paragrafo 3, lettera b), del paragrafo 3, lettera b), del paragrafo 4, lettera b), del paragrafo 5, lettera b), e del paragrafo 6, lettera b).

8. Gli Stati membri, l'unità centrale ETIAS ed Europol iniziano a utilizzare ciascuna delle componenti dell'interoperabilità a decorrere dalla data stabilita dalla Commissione ai sensi, rispettivamente, dei paragrafi 1, 2, 3 e 4.

Articolo 69

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 28, paragrafo 5, all'articolo 39, paragrafo 5, all'articolo 49, paragrafo 6, all'articolo 63, paragrafo 2, e all'articolo 65, paragrafo 8, è conferito alla Commissione per un periodo di cinque anni a decorrere dall'11 giugno 2019. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega dei poteri di cui all'articolo 28, paragrafo 5, all'articolo 39, paragrafo 5, all'articolo 49, paragrafo 6, all'articolo 63, paragrafo 2, e all'articolo 65, paragrafo 8, 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 28, paragrafo 5, dell'articolo 39, paragrafo 5, dell'articolo 49, paragrafo 6, dell'articolo 63, paragrafo 2, e dell'articolo 65, paragrafo 8, 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 70

Procedura di approvazione

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.

Qualora il comitato non esprima alcun parere, la Commissione non adotta il progetto di atto di esecuzione e si applica l'articolo 5, paragrafo 4, terzo comma, del regolamento (UE) n. 182/2011.

Articolo 71

Gruppo consultivo

eu-LISA istituisce un gruppo consultivo di interoperabilità. In fase di progettazione e di sviluppo delle componenti dell'interoperabilità si applica l'articolo 54, paragrafi 4, 5 e 6.

Articolo 72

Formazione

eu-LISA svolge compiti relativi all'offerta di formazione sull'uso tecnico delle componenti dell'interoperabilità a norma del regolamento (UE) 2018/1726.

Le autorità degli Stati membri e gli organi dell'Unione forniscono al loro personale autorizzato a trattare i dati utilizzando le componenti dell'interoperabilità un adeguato programma di formazione sulla sicurezza dei dati, la qualità dei dati, le norme in materia di protezione dei dati, le procedure applicabili al trattamento dei dati e gli obblighi d'informazione ai sensi degli articoli 32, paragrafo 4, 33, paragrafo 4, e 47.

Se del caso, sono organizzati corsi di formazione comuni a livello di Unione per rafforzare la cooperazione e lo scambio di migliori pratiche tra il personale delle autorità degli Stati membri e degli organi dell'Unione autorizzato a trattare i dati utilizzando le componenti dell'interoperabilità. È prestata particolare attenzione al processo di individuazione multipla dell'identità, compresa la verifica manuale delle identità diverse e la relativa necessità di mantenere idonee garanzie dei diritti fondamentali.

Articolo 73

Manuale pratico

La Commissione, in stretta cooperazione con gli Stati membri, eu-LISA e altre agenzie pertinenti dell'Unione, mette a disposizione un manuale pratico per l'implementazione e la gestione delle componenti dell'interoperabilità. Il manuale pratico fornisce orientamenti tecnici e operativi, raccomandazioni e migliori prassi. La Commissione adotta il manuale pratico sotto forma di raccomandazione.

Articolo 74

Monitoraggio e valutazione

1. eu-LISA provvede affinché siano istituite procedure per monitorare lo sviluppo delle componenti dell'interoperabilità e la loro connessione all'interfaccia uniforme nazionale rispetto agli obiettivi relativi alla pianificazione e ai costi, nonché per monitorare il funzionamento delle componenti dell'interoperabilità rispetto agli obiettivi prefissati in termini di risultati tecnici, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

2. Entro il 12 dicembre 2019 e successivamente ogni sei mesi durante la fase di sviluppo delle componenti, eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sulla situazione dello sviluppo delle componenti dell'interoperabilità nonché sulla loro connessione all'interfaccia uniforme nazionale. Una volta che lo sviluppo è completato, è presentata al Parlamento europeo e al Consiglio una relazione che illustra nel dettaglio il modo in cui sono stati conseguiti gli obiettivi, in particolare quelli relativi alla pianificazione e ai costi, giustificando eventuali scostamenti.

3. Quattro anni dopo l'entrata in funzione di ciascuna componente dell'interoperabilità a norma dell'articolo 68, e successivamente ogni quattro anni, eu-LISA presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico delle componenti dell'interoperabilità, compresa la loro sicurezza.

4. Un anno dopo ogni relazione di eu-LISA la Commissione effettua una valutazione globale delle componenti di interoperabilità, che comprende:

a) una valutazione dell'applicazione del presente regolamento;

b) un'analisi dei risultati conseguiti in relazione agli obiettivi del presente regolamento e della sua incidenza sui diritti fondamentali, compresa in particolare una valutazione dell'impatto delle componenti dell'interoperabilità sul diritto alla non discriminazione;

c) una valutazione del funzionamento del portale web, compresi dati relativi all'utilizzo del portale web e il numero di richieste risolte;

d) una valutazione della perdurante validità dei principi di base delle componenti dell'interoperabilità;

e) una valutazione della sicurezza delle componenti dell'interoperabilità;

f) una valutazione dell'uso del CIR a fini di identificazione;

g) una valutazione dell'uso del CIR a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi;

h) una valutazione delle eventuali implicazioni, incluso qualsiasi impatto sproporzionato sul flusso di traffico ai valichi di frontiera, e di quelle aventi un impatto sul bilancio generale dell'Unione;

i) una valutazione della ricerca nelle banche dati Interpol attraverso l'ESP che comprenda informazioni sul numero di riscontri ottenuti dalle banche dati Interpol e informazioni sugli eventuali problemi riscontrati.

La valutazione globale a norma del primo comma del presente paragrafo comprende le necessarie raccomandazioni. La Commissione trasmette la relazione di valutazione al Parlamento europeo, al Consiglio, al garante europeo della protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali.

5. Entro il 12 giugno 2020 e successivamente ogni anno fino all'adozione degli atti di esecuzione della Commissione di cui all'articolo 68, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sullo stato di avanzamento dei preparativi per la piena attuazione del presente regolamento. Tale relazione contiene anche informazioni particolareggiate sulle spese sostenute e sugli eventuali rischi che possono incidere sui costi complessivi.

6. Due anni dopo l'entrata in funzione del MID a norma dell'articolo 68, paragrafo 4, la Commissione effettua un esame dell'impatto del MID sul diritto alla non discriminazione. In seguito a questa prima relazione, l'esame dell'impatto del MID sul diritto alla non discriminazione deve far parte dell'esame di cui al paragrafo 4, lettera b) del presente articolo.

7. Gli Stati membri ed Europol comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi da 3 a 6. Tali informazioni non mettono a repentaglio i metodi di lavoro né comprendono indicazioni sulle fonti, sui membri del personale o sulle indagini delle autorità designate.

8. eu-LISA comunica alla Commissione le informazioni necessarie per redigere le valutazioni comprensive di cui al paragrafo 4.

9. Nel rispetto delle disposizioni del diritto nazionale relative alla pubblicazione di informazioni sensibili, e fatte salve le limitazioni necessarie per tutelare la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non sia compromessa alcuna indagine nazionale, ciascuno Stato membro ed Europol predispongono relazioni annuali sull'efficacia dell'accesso ai dati conservati nel CIR a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, in cui figurino informazioni e statistiche su quanto segue:

a) gli scopi esatti delle consultazioni, compresi i tipi di reati di terrorismo o altri reati gravi;

b) i fondati motivi addotti per il sospetto fondato che l'autore presunto o effettivo oppure la vittima rientri nell'ambito di applicazione del regolamento (UE) n. 603/2013;

c) il numero delle richieste di accesso al CIR a fini di prevenzione, accertamento e indagine di reati di terrorismo o altri reati gravi;

d) il numero e i tipi di casi in cui si è giunti a un'identificazione;

e) la necessità di trattare casi eccezionali d'urgenza, compresi i casi in cui il punto di accesso centrale non ha confermato l'urgenza dopo la verifica a posteriori.

Le relazioni annuali preparate dagli Stati membri e da Europol sono trasmesse alla Commissione entro il 30 giugno dell'anno successivo.

10. Una soluzione tecnica è messa a disposizione degli Stati membri per gestire le richieste di accesso dell'utente di cui all'articolo 22 e agevolare la raccolta delle informazioni a norma dei paragrafi 7 e 9 del presente articolo ai fini dell'elaborazione delle relazioni e delle statistiche di cui a tali paragrafi. La Commissione adotta atti di esecuzione per fissare le specifiche della soluzione tecnica. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 70, paragrafo 2.

Articolo 75

Entrata in vigore e applicazione

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

Le disposizioni del presente regolamento relative all'ESP si applicano a decorrere dalla data determinata dalla Commissione a norma dell'articolo 68, paragrafo 1.

Le disposizioni del presente regolamento relative al BMS comune si applicano a decorrere dalla data determinata dalla Commissione a norma dell'articolo 68, paragrafo 2.

Le disposizioni del presente regolamento relative al CIR si applicano a decorrere dalla data determinata dalla Commissione a norma dell'articolo 68, paragrafo 3.

Le disposizioni del presente regolamento relative al MID si applicano a decorrere dalla data determinata dalla Commissione a norma dell'articolo 68, paragrafo 4.

Le disposizioni del presente regolamento relative ai meccanismi e alle procedure di controllo della qualità dei dati automatizzati, agli indicatori comuni di qualità dei dati e alle norme minime di qualità si applicano a decorrere dalle date rispettivamente determinate dalla Commissione a norma dell'articolo 68, paragrafo 5.

Le disposizioni del presente regolamento relative al CRRS si applicano a decorrere dalla data stabilita dalla Commissione all'articolo 68, paragrafo 6.

Gli articoli 6, 12, 17, 25, 38, 42, 52, 54, 56, 58, 66, 67, 69, 70, 71, 73 e 74, paragrafo 1, si applicano a decorrere dall'11 giugno 2019.

Il presente regolamento si applica in relazione all'Eurodac a decorrere dalla data in cui la rifusione del regolamento (UE) n. 603/2013 diventa applicabile.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri conformemente ai trattati.

Fatto a Bruxelles, il 20 maggio 2019

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
A. TAJANI	G. CIAMBA

ISSN 1977-0707 (edizione elettronica)
ISSN 1725-258X (edizione cartacea)

Ufficio delle pubblicazioni dell'Unione europea
2985 Lussemburgo
LUSSEMBURGO

IT