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