

## I

(Atti legislativi)

## REGOLAMENTI

## 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 (rifusione)**

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 78, paragrafo 2, lettera e), l'articolo 87, paragrafo 2, lettera a), e l'articolo 88, paragrafo 2, lettera a),

vista la proposta della Commissione europea,

visto il parere del garante europeo della protezione dei dati <sup>(1)</sup>,

deliberando secondo la procedura legislativa ordinaria <sup>(2)</sup>,

considerando quanto segue:

(1) È necessario apportare una serie di modifiche sostanziali al regolamento (CE) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino <sup>(3)</sup> e al regolamento (CE) n. 407/2002 del Consiglio, del 28 febbraio 2002, che definisce talune modalità di applicazione del regolamento (CE) n. 2725/2000 che istituisce l'"Eurodac" per il con-

fronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino <sup>(4)</sup>. È quindi opportuno provvedere, per ragioni di chiarezza, alla rifusione di tali regolamenti.

(2) Una politica comune nel settore dell'asilo, che preveda un sistema europeo comune di asilo, costituisce un elemento fondamentale dell'obiettivo dell'Unione europea relativo alla progressiva realizzazione di uno spazio di libertà, sicurezza e giustizia aperto a quanti, spinti dalle circostanze, cercano protezione internazionale nell'Unione.

(3) Il 4 novembre 2004 il Consiglio europeo ha adottato il programma dell'Aia, che ha fissato gli obiettivi da conseguire nel periodo 2005-2010 nello spazio di libertà, sicurezza e giustizia. Il patto europeo sull'immigrazione e l'asilo, approvato dal Consiglio europeo del 15-16 ottobre 2008, ha chiesto il completamento dell'istituzione del sistema europeo comune di asilo introducendo una procedura unica, che preveda garanzie comuni e uno status uniforme per i rifugiati e per le persone aventi titolo a beneficiare della protezione sussidiaria.

(4) Ai fini dell'applicazione del regolamento (UE) n. 604/2013 del Parlamento europeo e del Consiglio, del 26 giugno 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 <sup>(5)</sup>, è necessario determinare l'identità dei richiedenti protezione internazionale e delle persone fermate in relazione all'attraversamento

<sup>(1)</sup> GU C 92 del 10.4.2010, pag. 1.

<sup>(2)</sup> Posizione del Parlamento europeo del 12 giugno 2013 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 20 giugno 2013.

<sup>(3)</sup> GU L 316 del 15.12.2000, pag. 1.

<sup>(4)</sup> GU L 62 del 5.3.2002, pag. 1.

<sup>(5)</sup> Cfr. la pagina 31 della presente Gazzetta ufficiale.

irregolare delle frontiere esterne dell'Unione. È inoltre auspicabile, ai fini di un'efficace applicazione del regolamento (UE) n. 604/2013 e, in particolare, dell'articolo 18, paragrafo 1, lettere b) e d), consentire a ciascuno Stato membro di accertare se un cittadino di un paese terzo o un apolide trovato in condizioni di soggiorno irregolare nel suo territorio abbia presentato domanda di protezione internazionale in un altro Stato membro.

- (5) Costituendo le impronte digitali un elemento importante per la determinazione dell'identità esatta di tali persone, occorre istituire un sistema per il confronto dei dati relativi alle loro impronte digitali.
- (6) A tal fine, è necessario istituire un sistema denominato 'Eurodac', comprendente un sistema centrale, che gestirà una banca dati centrale informatizzata di dati relativi alle impronte digitali, e i mezzi telematici necessari per le trasmissioni tra gli Stati membri e il sistema centrale ("infrastruttura di comunicazione").
- (7) Il programma dell'Aia ha sollecitato il miglioramento dell'accesso agli archivi di dati esistenti nell'Unione. Inoltre, il programma di Stoccolma ha auspicato una raccolta di dati ben mirata e uno sviluppo dello scambio di informazioni e dei relativi strumenti, dettato dalle esigenze in materia di applicazione della legge.
- (8) Nella lotta al terrorismo e ad altri reati gravi è essenziale che le autorità di contrasto dispongano delle informazioni più complete e aggiornate possibili per poter svolgere i loro compiti. Le informazioni contenute nell'Eurodac sono necessarie a fini di prevenzione, accertamento o indagine di reati di terrorismo di cui alla decisione quadro 2002/475/GAI del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo <sup>(1)</sup>, o di altri reati gravi di cui alla decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri <sup>(2)</sup>. È pertanto necessario che i dati dell'Eurodac siano messi a disposizione delle autorità designate dagli Stati membri e dell'Ufficio europeo di polizia (Europol) a fini di confronto, nel rispetto delle condizioni previste dal presente regolamento.
- (9) I poteri conferiti alle autorità di contrasto di accedere all'Eurodac dovrebbero lasciare impregiudicato il diritto di un richiedente protezione internazionale di vedere esaminata la propria domanda a tempo debito conformemente al diritto vigente. Inoltre, anche l'eventuale seguito dato dopo aver ottenuto una "risposta pertinente" dall'Eurodac dovrebbe lasciare impregiudicato tale diritto.
- (10) La Commissione, nella sua comunicazione al Consiglio e al Parlamento europeo, del 24 novembre 2005, concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra le banche dati europee nel settore della giustizia e degli affari interni, ritiene che le autorità incaricate della sicurezza interna potrebbero accedere all'Eurodac in casi ben definiti, qualora vi sia il fondato sospetto che l'autore di un reato di terrorismo o altro reato grave abbia presentato domanda di protezione internazionale. In detta comunicazione la Commissione dichiara inoltre che, ai fini del rispetto del principio di proporzionalità, occorre che l'Eurodac sia interrogato a questo scopo soltanto quando prevalga l'interesse della sicurezza pubblica, vale a dire qualora il reato o l'atto terroristico del quale si cerca di identificare l'autore sia così riprovevole da giustificare l'interrogazione di una banca dati contenente dati relativi a persone con la fedina penale pulita, e conclude che i limiti che le autorità responsabili della sicurezza interna devono rispettare per poter consultare l'Eurodac devono pertanto essere sempre molto più elevati rispetto a quelli fissati per l'interrogazione di banche dati giudiziarie.
- (11) Inoltre, Europol svolge un ruolo fondamentale nell'ambito della cooperazione tra le autorità degli Stati membri nel settore dell'investigazione di reati transfrontalieri, contribuendo alla prevenzione, all'analisi e all'indagine di attività criminali su scala europea. Pertanto, anche Europol dovrebbe avere accesso all'Eurodac nel quadro dei suoi compiti e in conformità della decisione 2009/371/GAI del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di polizia (Europol) <sup>(3)</sup>.
- (12) Le richieste di confronto con i dati Eurodac da parte di Europol dovrebbero essere autorizzate unicamente in casi specifici, in circostanze ben definite e sotto rigide condizioni.
- (13) Poiché l'Eurodac è stato originariamente istituito per agevolare l'applicazione della convenzione di Dublino, l'accesso all'Eurodac al fine di prevenire, accertare o indagare reati di terrorismo o altri reati gravi costituisce una nuova finalità rispetto a quella iniziale, nonché un'ingerenza nel diritto fondamentale al rispetto della vita privata di coloro i cui dati personali sono trattati nell'Eurodac. Un'ingerenza di questo tipo deve essere prevista dalla legge, che deve essere formulata con precisione sufficiente a consentire all'individuo di adeguare il proprio comportamento, e deve tutelare dall'arbitrarietà e indicare con sufficiente chiarezza il potere discrezionale conferito alle autorità competenti e il modo in cui tale potere è esercitato. In una società democratica qualunque ingerenza deve essere necessaria per proteggere un interesse legittimo e proporzionato e deve essere commisurata all'obiettivo legittimo che intende perseguire.
- (14) La finalità iniziale dell'istituzione dell'Eurodac non rendeva necessario prevedere la possibilità di chiedere confronti con la banca dati sulla base di un'impronta digitale

<sup>(1)</sup> GU L 164 del 22.6.2002, pag. 3.

<sup>(2)</sup> GU L 190 del 18.7.2002, pag. 1.

<sup>(3)</sup> GU L 121 del 15.5.2009, pag. 37.

latente, vale a dire di una traccia dattiloscopica rilevabile sul luogo del reato; tale possibilità è tuttavia fondamentale nel settore della cooperazione di polizia. La possibilità di confrontare un'impronta digitale latente con i dati relativi alle impronte digitali conservati nell'Eurodac, nei casi in cui si può ragionevolmente ritenere che l'autore o la vittima di un reato possano rientrare in una delle categorie contemplate dal presente regolamento, rappresenta, per le autorità designate dagli Stati membri, uno strumento utilissimo per la prevenzione, l'accertamento o l'indagine di reati di terrorismo o di altri reati gravi, quando per esempio l'unica prova disponibile sul luogo del reato consiste nelle impronte latenti.

- (15) Il presente regolamento stabilisce altresì le condizioni alle quali dovrebbero essere autorizzate le richieste di confronto dei dati relativi alle impronte digitali con i dati Eurodac a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, e le garanzie necessarie per assicurare la tutela del diritto fondamentale al rispetto della vita privata di coloro i cui dati personali sono trattati nell'Eurodac. Il rigore di dette condizioni rispecchia il fatto che la banca dati Eurodac registra i dati relativi alle impronte digitali di persone che non si presume abbiano commesso un reato di terrorismo o un altro reato grave.
- (16) Per assicurare la parità di trattamento di tutti i richiedenti e beneficiari di protezione internazionale, e per garantire la coerenza con l'acquis dell'Unione vigente in materia di asilo, in particolare con la direttiva 2011/95/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, recante norme sull'attribuzione, a cittadini di paesi terzi o apolidi, della qualifica di beneficiario di protezione internazionale, su uno status uniforme per i rifugiati o per le persone aventi titolo a beneficiare della protezione sussidiaria, nonché sul contenuto della protezione riconosciuta<sup>(1)</sup>, e con il regolamento (UE) n. 604/2013 è opportuno estendere l'ambito di applicazione del presente regolamento al fine di includervi i richiedenti protezione sussidiaria e i le persone aventi titolo a beneficiare di tale protezione.
- (17) È altresì necessario invitare gli Stati membri a rilevare e trasmettere tempestivamente i dati relativi alle impronte digitali di tutti i richiedenti protezione internazionale e di tutti i cittadini di paesi terzi e gli apolidi che vengano fermati in relazione all'attraversamento irregolare di una frontiera esterna di uno Stato membro, qualora costoro abbiano almeno 14 anni.
- (18) È necessario dettare disposizioni precise in ordine alla trasmissione al sistema centrale dei dati relativi a tali impronte digitali, alla registrazione, nel sistema centrale, dei dati suddetti e di altri dati pertinenti, alla loro memorizzazione, al loro confronto con altri dati relativi a impronte digitali, nonché in ordine alla trasmissione dei risultati di tali confronti e al contrassegno ed alla cancellazione dei dati registrati. Dette disposizioni possono

differire ed essere specificamente adattate per quanto riguarda altre categorie di cittadini di paesi terzi o apolidi.

- (19) Gli Stati membri dovrebbero assicurare la trasmissione di dati relativi alle impronte digitali di qualità adeguata ai fini del confronto mediante il sistema informatizzato per il riconoscimento delle impronte digitali. È opportuno che tutte le autorità aventi diritto di accesso all'Eurodac investano in idonee iniziative di formazione e nelle necessarie attrezzature tecniche. Le autorità aventi diritto di accesso all'Eurodac dovrebbero comunicare all'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, istituita dal regolamento (UE) n. 1077/2011 del Parlamento europeo e del Consiglio<sup>(2)</sup> (l'"Agenzia"), le difficoltà specifiche incontrate con riguardo alla qualità dei dati, onde consentire di porvi rimedio.
- (20) Il fatto che sia temporaneamente o permanentemente impossibile rilevare e/o trasmettere i dati relativi alle impronte digitali di una persona, per ragioni quali la qualità insufficiente dei dati ai fini di un confronto adeguato, problemi tecnici o motivi connessi alla tutela della salute, o che la persona interessata sia priva della capacità o della possibilità di far rilevare le proprie impronte digitali a causa di circostanze che esulano dal suo controllo, non influisce negativamente sull'esame o sulla decisione concernenti la domanda di protezione internazionale presentata da tale persona.
- (21) È opportuno che le risposte pertinenti ottenute dall'Eurodac siano verificate da un esperto avente una formazione specifica in dattiloscopia in modo da garantire l'esatta determinazione della competenza ai sensi del regolamento (UE) n. 604/2013 e la corretta identificazione dell'autore presunto o della vittima di un reato i cui dati potrebbero figurare nell'Eurodac.
- (22) I cittadini di paesi terzi e gli apolidi che hanno presentato domanda di protezione internazionale in uno Stato membro possono avere la possibilità di chiedere protezione internazionale per vari anni ancora in un altro Stato membro. Pertanto, il periodo massimo durante il quale le impronte digitali dovrebbero essere conservate dal sistema centrale dovrebbe essere piuttosto lungo. Dato che la maggior parte dei cittadini di paesi terzi e degli apolidi che hanno soggiornato nell'Unione per vari anni avranno ottenuto uno status giuridico definito ovvero avranno persino acquisito la cittadinanza di uno Stato membro al termine di tale periodo, si ritiene che dieci anni costituiscano un periodo ragionevole per la conservazione dei dati relativi alle impronte digitali.
- (23) Il periodo di conservazione dovrebbe essere ridotto in talune situazioni particolari in cui non vi sia necessità di conservare i dati dattiloscopici così a lungo. I dati dattiloscopici dovrebbero essere cancellati non appena i cittadini di paesi terzi e gli apolidi cui tali dati si riferiscono acquisiscono la cittadinanza di uno Stato membro.

<sup>(1)</sup> GU L 337 del 20.12.2011, pag. 9.

<sup>(2)</sup> GU L 286 dell'1.11.2011, pag. 1.

- (24) È opportuno conservare i dati di coloro le cui impronte digitali sono state inizialmente registrate nell'Eurodac al momento della presentazione della domanda di protezione internazionale e ai quali è stata riconosciuta la protezione in uno Stato membro, al fine di consentire il confronto di detti dati con quelli registrati al momento della presentazione di una domanda di protezione internazionale.
- (25) L'agenzia è stata incaricata di svolgere i compiti della Commissione relativi alla gestione operativa dell'Eurodac ai sensi del presente regolamento, nonché di determinati aspetti dell'infrastruttura di comunicazione a decorrere dalla data in cui l'agenzia è entrata in funzione il 1° dicembre 2012. L'agenzia dovrebbe assumere i compiti ad essa conferiti dal presente regolamento e le disposizioni in materia del regolamento (UE) n. 1077/2011 dovrebbero essere modificate di conseguenza. Inoltre, Europol dovrebbe beneficiare dello status di osservatore alle riunioni del consiglio di amministrazione dell'agenzia quando è all'ordine del giorno una questione relativa all'applicazione del presente regolamento riguardante l'accesso per la consultazione dell'Eurodac da parte delle autorità designate dagli Stati membri e di Europol a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi. È opportuno che Europol possa nominare un rappresentante in seno al gruppo consultivo Eurodac dell'agenzia.
- (26) Lo statuto dei funzionari dell'Unione europea ("statuto dei funzionari") e il regime applicabile agli altri agenti dell'Unione europea ("regime applicabile"), stabiliti con regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio <sup>(1)</sup> (indicati complessivamente come "statuto dei funzionari"), dovrebbero applicarsi a tutti i membri del personale dell'agenzia che si occupano di questioni attinenti al presente regolamento.
- (27) È necessario precisare chiaramente le competenze rispettive della Commissione e dell'agenzia, nei riguardi del sistema centrale e dell'infrastruttura di comunicazione, e degli Stati membri, per quanto concerne il trattamento, la sicurezza, l'accesso e la rettifica dei dati registrati.
- (28) È necessario designare le autorità competenti degli Stati membri e il punto di accesso nazionale attraverso i quali sono inoltrate le richieste di confronto con i dati Eurodac, e conservare un elenco delle unità operative in seno alle autorità designate autorizzate a chiedere tale confronto ai fini specifici della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o di altri reati gravi.
- (29) Le richieste di confronto con i dati conservati nel sistema centrale dovrebbero essere presentate dalle unità operative in seno alle autorità designate al punto di accesso nazionale attraverso l'autorità di verifica e dovrebbero essere motivate. Le unità operative in seno alle autorità designate che sono autorizzate a chiedere i confronti con i dati Eurodac non dovrebbero agire in qualità di autorità di verifica. Le autorità di verifica dovrebbero agire in piena indipendenza rispetto alle autorità designate e dovrebbero assicurare, in modo indipendente, l'assoluta conformità alle condizioni di accesso previste nel presente regolamento, per poi trasmettere la richiesta di confronto, senza comunicare le ragioni della medesima, al sistema centrale attraverso il punto di accesso nazionale, previa verifica del rispetto di tutte le condizioni di accesso. In casi eccezionali di urgenza in cui sia necessario un accesso tempestivo per rispondere a una minaccia specifica e reale connessa a reati di terrorismo o altri reati gravi, l'autorità di verifica dovrebbe trattare la richiesta immediatamente ed effettuare la verifica a posteriori.
- (30) L'autorità designata e l'autorità di verifica possono far parte della stessa organizzazione se il diritto nazionale lo consente, ma l'autorità di verifica dovrebbe agire con indipendenza quando svolge i propri compiti ai sensi del presente regolamento.
- (31) Ai fini della protezione dei dati personali e per escludere confronti sistematici, che dovrebbero essere vietati, il trattamento dei dati Eurodac dovrebbe avvenire solo in casi specifici e quando necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi. Costituisce un caso specifico il fatto che la richiesta di confronto sia connessa a un evento specifico e concreto o a un pericolo specifico e concreto associato a un reato di terrorismo o a un altro reato grave, oppure a persone specifiche nei cui confronti sussistano fondati motivi di ritenere che intendano commettere o abbiano commesso un tale reato. Un altro caso specifico è quello in cui la richiesta di confronto è connessa a una persona che è vittima di un reato di terrorismo o altro reato grave. Le autorità designate ed Europol dovrebbero pertanto chiedere un confronto con Eurodac soltanto quando hanno fondati motivi per ritenere che tale confronto fornisca informazioni che contribuiranno in modo sostanziale alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o altri reati gravi.
- (32) Inoltre, l'accesso dovrebbe essere consentito soltanto a condizione che i confronti con le banche dati nazionali d'identificazione dattiloscopica degli Stati membri e con i sistemi automatizzati d'identificazione dattiloscopica di tutti gli altri Stati membri ai sensi della decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera <sup>(2)</sup>, non consentano di stabilire l'identità della persona interessata. Tale condizione richiede che lo Stato membro richiedente esegua confronti con i sistemi automatizzati d'identificazione dattiloscopica di tutti gli altri Stati membri ai sensi della decisione 2008/615/GAI che sono tecnicamente disponibili, a meno che detto Stato membro non possa dimostrare che esistono fondati motivi per ritenere che ciò non consentirebbe di stabilire

<sup>(1)</sup> GU L 56 del 4.3.1968, pag. 1.

<sup>(2)</sup> GU L 210 del 6.8.2008, pag. 1.

l'identità della persona interessata. Tali fondati motivi esistono in particolare quando il caso specifico non presenta alcun legame operativo o investigativo con un dato Stato membro. Tale condizione richiede la preventiva attuazione giuridica e tecnica della decisione 2008/615/GAI da parte dello Stato membro richiedente nel campo dei dati relativi alle impronte digitali, poiché non dovrebbe essere consentito svolgere un controllo nell'ambito dell'Eurodac a fini di contrasto senza aver prima adottato le disposizioni di cui sopra.

- (33) Prima di cercare sull'Eurodac le autorità designate dovrebbero inoltre, purché siano soddisfatte le condizioni per un confronto, consultare il sistema di informazione visti ai sensi della 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 <sup>(1)</sup>.
- (34) Ai fini di un confronto e di uno scambio di dati personali efficaci, gli Stati membri dovrebbero attuare e applicare pienamente gli accordi internazionali esistenti nonché il diritto dell'Unione in materia di scambio di dati personali già in vigore, in particolare la decisione 2008/615/GAI.
- (35) L'interesse superiore del minore dovrebbe costituire una considerazione preminente per gli Stati membri in sede di attuazione del presente regolamento. Qualora lo Stato membro richiedente stabilisca che i dati Eurodac si riferiscono a un minore, tali dati possono essere utilizzati soltanto a fini di contrasto dallo Stato membro richiedente nel rispetto del proprio diritto applicabile ai minori e conformemente all'obbligo di considerare in primo luogo l'interesse superiore del minore.
- (36) Mentre la responsabilità extracontrattuale dell'Unione in relazione alle attività del sistema Eurodac sarà disciplinata dalle pertinenti disposizioni del trattato sul funzionamento dell'Unione europea (TFUE), è necessario dettare regole specifiche per la responsabilità extracontrattuale degli Stati membri in relazione al funzionamento del sistema.
- (37) Poiché l'obiettivo del presente regolamento, vale a dire l'istituzione di un sistema per il confronto dei dati relativi alle impronte digitali come supporto all'attuazione della politica di asilo dell'Unione, non può, per sua stessa natura, essere conseguito in misura sufficiente dagli Stati membri e può dunque 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.

- (38) La direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati <sup>(2)</sup>, si applica al trattamento dei dati personali effettuato dagli Stati membri in applicazione del presente regolamento, a meno che tale trattamento sia effettuato dalle autorità designate o dalle autorità di verifica degli Stati membri a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi.
- (39) I trattamenti di dati personali effettuati dalle autorità degli Stati membri a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi in conformità del presente regolamento dovrebbero essere soggetti a standard di protezione dei dati personali ai sensi del rispettivo diritto nazionale conformi alla decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale <sup>(3)</sup>.
- (40) I principi sanciti dalla direttiva 95/46/CE in tema di protezione dei diritti e delle libertà delle persone fisiche, in particolare il loro diritto alla tutela della vita privata, con riguardo al trattamento dei dati personali, andrebbero rafforzati o chiariti, in particolare in rapporto ad alcuni settori.
- (41) È opportuno vietare il trasferimento dei dati personali ottenuti da uno Stato membro o da Europol ai sensi del presente regolamento dal sistema centrale a qualunque paese terzo, organizzazione internazionale o soggetto di diritto privato con sede nell'Unione o fuori di essa, onde garantire il diritto di asilo e tutelare i richiedenti protezione internazionale dalla divulgazione dei loro dati a paesi terzi. Ciò significa che gli Stati membri non dovrebbero trasferire informazioni ottenute dal sistema centrale concernenti: lo Stato membro o gli Stati membri d'origine; il luogo e la data in cui è stata presentata la domanda di protezione internazionale; il numero di riferimento assegnato dallo Stato membro d'origine; la data di rilevamento delle impronte digitali nonché la data in cui lo Stato membro o gli Stati membri hanno trasmesso i dati all'Eurodac; l'identificativo utente dell'operatore; e qualunque informazione relativa a un trasferimento dell'interessato ai sensi del regolamento (UE) n. 604/2013. Tale divieto non dovrebbe pregiudicare il diritto degli Stati membri di trasferire tali dati a paesi terzi cui si applica il regolamento (UE) n. 604/2013 in modo che gli Stati membri possano cooperare con quei paesi terzi ai fini del presente regolamento.

<sup>(1)</sup> GU L 218 del 13.8.2008, pag. 129.

<sup>(2)</sup> GU L 281 del 23.11.1995, pag. 31.

<sup>(3)</sup> GU L 350 del 30.12.2008, pag. 60.

- (42) Le autorità nazionali di controllo dovrebbero vigilare sulla liceità del trattamento dei dati personali effettuato dagli Stati membri, mentre l'autorità di controllo istituita dalla decisione 2009/371/GAI dovrebbe vigilare sulla liceità delle attività di trattamento dei dati eseguite da Europol.
- (43) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché alla libera circolazione di tali dati <sup>(1)</sup>, in particolare gli articoli 21 e 22 sulla riservatezza e sulla sicurezza del trattamento, si applica al trattamento dei dati personali effettuato da istituzioni, organi e organismi dell'Unione in applicazione del presente regolamento. Occorre tuttavia precisare taluni punti per quanto concerne la responsabilità in materia di trattamento dei dati e il controllo della protezione degli stessi, tenendo presente che la protezione dei dati è un fattore chiave per il successo operativo dell'Eurodac e che la sicurezza dei dati, l'alta qualità tecnica e la legittimità della consultazione sono elementi essenziali per assicurare il regolare e corretto funzionamento dell'Eurodac nonché per facilitare l'applicazione del regolamento (UE) n. 604/2013
- (44) L'interessato dovrebbe essere informato dello scopo per cui i suoi dati saranno trattati nell'ambito dell'Eurodac nonché ricevere una descrizione delle finalità del regolamento (UE) n. 604/2013 e dell'uso che le autorità di contrasto possono fare dei suoi dati.
- (45) È opportuno che le autorità nazionali di controllo verifichino la liceità del trattamento dei dati personali effettuato dagli Stati membri e che il garante europeo della protezione dei dati, di cui al regolamento (CE) n. 45/2001, controlli le attività delle istituzioni, degli organi e degli organismi dell'Unione attinenti al trattamento dei dati personali effettuato ai sensi del presente regolamento.
- (46) Gli Stati membri, il Parlamento europeo, il Consiglio e la Commissione dovrebbero garantire che le autorità di controllo nazionali ed europee siano in grado di controllare adeguatamente l'uso dei dati Eurodac e l'accesso ai medesimi.
- (47) È opportuno controllare e valutare l'attività dell'Eurodac a intervalli regolari, onde stabilire, fra l'altro, se l'accesso a fini di contrasto determini una discriminazione indiretta nei confronti dei richiedenti protezione internazionale, come indicato nella valutazione della Commissione in merito alla conformità del presente regolamento con la Carta dei diritti fondamentali dell'Unione europea ("la Carta"). L'agenzia dovrebbe trasmettere annualmente al Parlamento europeo e al Consiglio una relazione sulle attività del sistema centrale.
- (48) Gli Stati membri dovrebbero istituire un sistema di sanzioni efficaci, proporzionate e dissuasive per punire il trattamento dei dati inseriti nel sistema centrale con finalità contrarie a quelle dell'Eurodac.
- (49) È necessario che gli Stati membri siano informati della situazione di determinate procedure di asilo onde facilitare un'adeguata applicazione del regolamento (UE) n. 604/2013
- (50) Il presente regolamento rispetta i diritti fondamentali e osserva i principi sanciti segnatamente nella Carta. In particolare, il presente regolamento intende assicurare il pieno rispetto della protezione dei dati personali e del diritto di richiedere protezione internazionale nonché promuovere l'applicazione degli articoli 8 e 18 della Carta. Il presente regolamento dovrebbe pertanto essere applicato di conseguenza.
- (51) 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.
- (52) 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 che desidera partecipare all'adozione e all'applicazione del presente regolamento.
- (53) 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.
- (54) È opportuno far coincidere l'ambito di applicazione territoriale del presente regolamento con quello del regolamento (UE) n. 604/2013,

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

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

## CAPO I

### DISPOSIZIONI GENERALI

#### Articolo 1

#### Scopo dell'"Eurodac"

1. È istituito un sistema denominato "Eurodac", allo scopo di concorrere alla determinazione dello Stato membro competente, ai sensi del regolamento (UE) n. 604/2013, per l'esame di una domanda di protezione internazionale presentata in uno Stato membro da un cittadino di un paese terzo o da un apolide, e di facilitare inoltre l'applicazione del regolamento (UE) n. 604/2013 secondo le condizioni stabilite dal presente regolamento.

2. Il presente regolamento stabilisce inoltre le condizioni per le richieste di confronto dei dati relativi alle impronte digitali con i dati conservati nel sistema centrale, presentate dalle autorità designate degli Stati membri e dall'Ufficio europeo di polizia (Europol) a fini di contrasto.

3. Fatto salvo il trattamento dei dati destinati all'Eurodac da parte dello Stato membro d'origine in banche dati istituite ai sensi del proprio diritto nazionale, i dati relativi alle impronte digitali e gli altri dati personali possono essere trattati nell'Eurodac solo per gli scopi previsti dal presente regolamento e dall'articolo 34, paragrafo 1, del regolamento UE n. 604/2013.

#### Articolo 2

#### Definizioni

1. Ai fini del presente regolamento si intende per:

a) "richiedente protezione internazionale": il cittadino di un paese terzo o l'apolide che abbia manifestato la volontà di chiedere protezione internazionale ai sensi dell'articolo 2, lettera h), della direttiva 2011/95/UE, sulla quale non sia stata ancora adottata una decisione definitiva;

b) "Stato membro d'origine":

i) in relazione alle persone di cui all'articolo 9, paragrafo 1, lo Stato membro che trasmette i dati personali al sistema centrale e che riceve i risultati del confronto;

ii) in relazione alle persone di cui all'articolo 14, paragrafo 1, lo Stato membro che trasmette i dati personali al sistema centrale;

iii) in relazione alle persone di cui all'articolo 17, paragrafo 1, lo Stato membro che trasmette detti dati al sistema centrale e che riceve i risultati del confronto;

c) "beneficiario di protezione internazionale": il cittadino di un paese terzo o l'apolide al quale è stato riconosciuto il diritto alla protezione internazionale quale definita all'articolo 2, lettera a), della direttiva 2011/95/UE;

d) "risposta pertinente": la corrispondenza constatata o le corrispondenze constatate dal sistema centrale, sulla base di un confronto, tra i dati relativi alle impronte digitali registrati nella banca dati centrale informatizzata e quelli trasmessi da uno Stato membro relativi a una persona, fatto salvo l'obbligo degli Stati membri di controllare immediatamente l'esito del confronto a norma dell'articolo 25, paragrafo 4;

e) "punto di accesso nazionale": il sistema nazionale designato per comunicare con il sistema centrale;

f) "agenzia": l'agenzia istituita con regolamento (UE) n. 1077/2011;

g) "Europol": l'Ufficio europeo di polizia istituito con decisione 2009/371/GAI;

h) "dati Eurodac": tutti i dati conservati nel sistema centrale conformemente all'articolo 11 e all'articolo 14, paragrafo 2;

i) "contrasto": la prevenzione, l'accertamento o l'indagine di reati di terrorismo o di altri reati gravi;

j) "reati di terrorismo": i reati che, ai sensi del diritto nazionale, corrispondono o sono equivalenti a quelli di cui agli articoli da 1 a 4 della decisione quadro 2002/475/GAI;

k) "reati gravi": le forme di reato che corrispondono o sono equivalenti a quelle di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI, se punibili 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;

l) "dati relativi alle impronte digitali": i dati sulle impronte digitali di tutte le dita o almeno degli indici e, qualora queste ultime non fossero disponibili, sulle impronte di tutte le altre dita, oppure un'impronta digitale latente.

2. I termini definiti nell'articolo 2 della direttiva 95/46/CE hanno lo stesso significato nel presente regolamento, nella misura in cui i dati personali siano trattati dalle autorità degli Stati membri ai fini di cui all'articolo 1, paragrafo 1, del presente regolamento.

3. Salvo diverse disposizioni, i termini definiti nell'articolo 2 del regolamento (UE) n. 604/2013 hanno lo stesso significato nel presente regolamento.

4. I termini definiti nell'articolo 2 della decisione quadro 2008/977/GAI hanno lo stesso significato nel presente regolamento laddove i dati personali siano trattati dalle autorità degli Stati membri ai fini di cui all'articolo 1, paragrafo 2, del presente regolamento.

### Articolo 3

#### Architettura del sistema e principi di base

1. L'Eurodac consta di:
  - a) una banca dati centrale informatizzata per le impronte digitali ("sistema centrale") costituita da:
    - i) un'unità centrale,
    - ii) un piano e un sistema di continuità operativa;
  - b) un'infrastruttura di comunicazione tra il sistema centrale e gli Stati membri, dotata di una rete virtuale cifrata dedicata ai dati Eurodac ("infrastruttura di comunicazione").
2. Ciascuno Stato membro dispone di un unico punto di accesso nazionale.
3. I dati riguardanti le persone di cui agli articoli 9, paragrafo 1, 14, paragrafo 1, e 17, paragrafo 1, sono trattati dal sistema centrale per conto dello Stato membro d'origine alle condizioni indicate nel presente regolamento e sono tenuti separati con mezzi tecnici adeguati.
4. Le norme cui è soggetto l'Eurodac si applicano anche alle operazioni effettuate dagli Stati membri dal momento della trasmissione dei dati al sistema centrale fino all'utilizzazione dei risultati del confronto.
5. La procedura di rilevamento delle impronte digitali è stabilita e applicata in conformità delle prassi nazionali dello Stato membro interessato e in conformità delle salvaguardie previste

dalla Carta dei diritti fondamentali dell'Unione europea, dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dalla Convenzione delle Nazioni Unite sui diritti del fanciullo.

### Articolo 4

#### Gestione operativa

1. L'agenzia è responsabile della gestione operativa dell'Eurodac.

La gestione operativa dell'Eurodac consiste nell'insieme dei compiti necessari a garantire un funzionamento dell'Eurodac 24 ore su 24 e 7 giorni su 7, ai sensi del presente regolamento, e comprende in particolare la manutenzione e gli adeguamenti tecnici necessari a garantire che il sistema funzioni a un livello di qualità operativa soddisfacente, specialmente per quanto riguarda il tempo richiesto per l'interrogazione del sistema centrale. Sono elaborati un piano e un sistema di continuità operativa che prendono in considerazione le esigenze di manutenzione e i periodi di inattività del sistema impreveduti, incluso l'impatto delle misure per la continuità operativa sulla protezione e sulla sicurezza dei dati.

In cooperazione con gli Stati membri, l'agenzia provvede a che in qualsiasi momento siano utilizzate, previa analisi costi/benefici, le migliori e più sicure tecnologie e tecniche disponibili per il sistema centrale.

2. L'agenzia è responsabile dei seguenti compiti relativi all'infrastruttura di comunicazione:

- a) controllo;
  - b) sicurezza;
  - c) coordinamento delle relazioni tra gli Stati membri e il gestore.
3. La Commissione è responsabile di tutti i compiti relativi all'infrastruttura di comunicazione diversi da quelli di cui al paragrafo 2, in particolare:
- a) l'esecuzione del bilancio;
  - b) acquisizione e rinnovo;
  - c) aspetti contrattuali.

4. Fatto salvo l'articolo 17 dello statuto dei funzionari, l'agenzia applica norme adeguate in materia di segreto professionale o altri doveri di riservatezza equivalenti a tutti i membri del proprio personale che devono lavorare con i dati Eurodac. Questo obbligo vincola tale personale anche dopo che abbia lasciato l'incarico o cessato di lavorare, ovvero portato a termine i suoi compiti.

#### Articolo 5

##### **Autorità designate degli Stati membri a fini di contrasto**

1. Ai fini di cui all'articolo 1, paragrafo 2, gli Stati membri designano le autorità autorizzate a chiedere il confronto con i dati Eurodac a norma del presente regolamento. Le autorità designate sono le autorità degli Stati membri responsabili della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o di altri reati gravi. Le autorità designate non includono le agenzie o le unità esclusivamente responsabili delle attività di intelligence concernenti la sicurezza nazionale.

2. Ciascuno Stato membro conserva un elenco delle autorità designate.

3. Ciascuno Stato membro conserva un elenco delle unità operative in seno alle autorità designate che possono chiedere il confronto con i dati Eurodac attraverso il punto di accesso nazionale.

#### Articolo 6

##### **Autorità di verifica degli Stati membri a fini di contrasto**

1. Ai fini di cui all'articolo 1, paragrafo 2, ciascuno Stato membro designa un'autorità nazionale unica o un'unità di tale autorità affinché eserciti le funzioni di autorità di verifica. L'autorità di verifica è l'autorità dello Stato membro responsabile della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o di altri reati gravi.

L'autorità designata e l'autorità di verifica possono far parte della stessa organizzazione se il diritto nazionale lo consente, ma l'autorità di verifica agisce indipendentemente nello svolgimento dei propri compiti ai sensi del presente regolamento. L'autorità di verifica è distinta dalle unità operative di cui all'articolo 5, paragrafo 3, e non riceve istruzioni dalle stesse in merito al risultato della verifica.

Gli Stati membri possono designare più di un'autorità di verifica al fine di rispecchiare le proprie strutture organizzative e amministrative, conformemente ai rispettivi obblighi costituzionali o giuridici.

2. Compete all'autorità di verifica garantire il rispetto delle condizioni per la richiesta di confronto delle impronte digitali con i dati Eurodac.

Soltanto il personale debitamente autorizzato dell'autorità di verifica è autorizzato a ricevere e a trasmettere una richiesta di accesso all'Eurodac ai sensi dell'articolo 19.

Soltanto l'autorità di verifica è autorizzata a trasmettere le richieste di confronto delle impronte digitali al punto di accesso nazionale.

#### Articolo 7

##### **Europol**

1. Ai fini di cui all'articolo 1, paragrafo 2, Europol designa un'unità specializzata composta di funzionari di Europol autorizzati ad agire in qualità di autorità di verifica, che agisce in piena indipendenza rispetto all'autorità designata di cui al paragrafo 2 del presente articolo quando svolge i propri compiti ai sensi del presente regolamento, e non riceve istruzioni dall'autorità designata in merito al risultato della verifica. Compete all'unità assicurarsi che siano rispettate le condizioni per la richiesta di confronto delle impronte digitali con i dati Eurodac. Europol, di concerto con ciascuno Stato membro, designa il punto di accesso nazionale di quello Stato membro che comunica al sistema centrale le sue richieste di confronto dei dati relativi alle impronte digitali.

2. Ai fini di cui all'articolo 1, paragrafo 2, Europol designa un'unità operativa autorizzata a chiedere il confronto con i dati Eurodac attraverso il suo punto di accesso nazionale. L'autorità designata è un'unità operativa di Europol competente per la raccolta, la conservazione, l'elaborazione, l'analisi e lo scambio di informazioni al fine di sostenere e potenziare l'azione degli Stati membri nel campo della prevenzione, dell'accertamento o dell'indagine di reati di terrorismo o di altri reati gravi che sono di competenza di Europol.

#### Articolo 8

##### **Statistiche**

1. Ogni tre mesi l'agenzia elabora una statistica sull'attività del sistema centrale da cui risultano in particolare:

- a) il numero dei dati trasmessi relativi alle persone di cui all'articolo 9, paragrafo 1, all'articolo 14, paragrafo 1, e all'articolo 17, paragrafo 1;
- b) il numero delle risposte pertinenti riguardanti i richiedenti protezione internazionale che hanno presentato domanda di protezione internazionale in un altro Stato membro;
- c) il numero delle risposte pertinenti riguardanti le persone di cui all'articolo 14, paragrafo 1, che hanno presentato domanda di protezione internazionale in un momento successivo;

- d) il numero delle risposte pertinenti riguardanti le persone di cui all'articolo 17, paragrafo 1, che hanno presentato in precedenza domanda di protezione internazionale in un altro Stato membro;
- e) il numero dei dati relativi alle impronte digitali che il sistema centrale ha dovuto richiedere più di una volta agli Stati membri di origine, in quanto i dati relativi alle impronte digitali trasmessi inizialmente non erano idonei al confronto mediante il sistema informatizzato per il riconoscimento delle impronte digitali;
- f) il numero delle serie di dati con contrassegno e senza contrassegno, congelate e sbloccate in conformità dell'articolo 18, paragrafi 1 e 3;
- g) il numero delle risposte pertinenti riguardanti le persone di cui all'articolo 18, paragrafo 1, per le quali erano state registrate risposte pertinenti ai sensi delle lettere b) e d) del presente articolo;
- h) il numero di richieste e di risposte pertinenti di cui all'articolo 20, paragrafo 1;
- i) il numero di richieste e di risposte pertinenti di cui all'articolo 21, paragrafo 1.

2. Alla fine di ogni anno viene elaborata una statistica in cui sono sintetizzati i dati delle statistiche trimestrali relative all'anno in questione e da cui risulta il numero delle persone nei cui confronti sono state constatate risposte pertinenti, ai sensi del paragrafo 1, lettere b), c) e d). La statistica contiene dati separati per ciascuno Stato membro. I risultati sono resi pubblici.

## CAPO II

### **RICHIEDENTI PROTEZIONE INTERNAZIONALE**

#### *Articolo 9*

#### **Rilevamento, trasmissione e confronto delle impronte digitali**

1. Ciascuno Stato membro procede tempestivamente al rilevamento delle impronte digitali di tutte le dita di ogni richiedente protezione internazionale di età non inferiore a 14 anni, non appena possibile e in ogni caso entro 72 ore dalla presentazione della domanda di protezione internazionale ai sensi dell'articolo 20, paragrafo 2, del regolamento (UE) n. 604/2013, trasmette tali dati al sistema centrale insieme ai dati di cui all'articolo 11, lettere da b) a g), del presente regolamento.

L'inosservanza del termine di 72 ore non dispensa gli Stati membri dal rilevare e trasmettere le impronte digitali al sistema centrale. Quando lo stato dei polpastrelli non consente di effettuare un rilevamento delle impronte di qualità tale da assicurare un confronto appropriato ai sensi dell'articolo 25, lo Stato membro d'origine provvede a rilevare nuovamente le impronte digitali del richiedente e le ritrasmette quanto prima e in ogni caso entro 48 ore dal buon esito del rilevamento.

2. In deroga al paragrafo 1, quando non è possibile rilevare le impronte digitali di un richiedente protezione internazionale a causa di provvedimenti che ne tutelano la salute o per motivi di salute pubblica, gli Stati membri rilevano e inviano tali impronte digitali quanto prima e in ogni caso entro 48 ore dal momento in cui tali motivi di salute sono venuti meno.

Nel caso di gravi problemi tecnici gli Stati membri possono prorogare di ulteriori 48 ore al massimo il termine di 72 ore di cui al paragrafo 1, al fine di attuare i piani di continuità nazionali.

3. I dati relativi alle impronte digitali di cui all'articolo 11, lettera a), trasmessi da qualsiasi Stato membro, a eccezione dei dati trasmessi a norma dell'articolo 10, lettera b), sono automaticamente confrontati con i dati relativi alle impronte digitali trasmessi da altri Stati membri e già registrati nel sistema centrale.

4. Il sistema centrale provvede affinché, su richiesta di uno Stato membro, il confronto di cui al paragrafo 3 venga effettuato con i dati relativi alle impronte digitali trasmessi precedentemente dallo stesso Stato membro, oltre che con i dati trasmessi dagli altri Stati membri.

5. Il sistema centrale trasmette automaticamente la risposta pertinente o il risultato negativo del confronto allo Stato membro d'origine. In caso di risposta pertinente vengono trasmessi, per tutte le serie di dati corrispondenti alla risposta pertinente, i dati di cui all'articolo 11, lettere da a) a k), insieme al contrassegno di cui all'articolo 18, paragrafo 1, se applicabile.

#### *Articolo 10*

#### **Informazioni sullo status dell'interessato**

Le seguenti informazioni sono inviate al sistema centrale e ivi conservate in conformità dell'articolo 12 ai fini della trasmissione di cui all'articolo 9, paragrafo 5:

- a) quando un richiedente protezione internazionale, o altro richiedente di cui all'articolo 18, paragrafo 1, lettera d), del regolamento (UE) n. 604/2013, giunge nello Stato membro competente in seguito a un trasferimento effettuato in forza di una decisione che acconsente a una richiesta di ripresa in carico di cui all'articolo 25 dello stesso, lo Stato membro competente aggiorna i dati registrati in conformità dell'articolo 11 del presente regolamento relativi all'interessato, aggiungendo la data di arrivo;
- b) quando un richiedente protezione internazionale giunge nello Stato membro competente in seguito a un trasferimento effettuato in forza di una decisione che acconsente a una richiesta di presa in carico di cui all'articolo 22 del regolamento (UE) n. 604/2013, lo Stato membro competente invia i dati registrati in conformità dell'articolo 11 del presente regolamento relativi all'interessato, e include la data di arrivo;

- c) non appena stabilisce che l'interessato, i cui dati sono stati registrati nell'Eurodac ai sensi dell'articolo 11 del presente regolamento, ha lasciato il territorio degli Stati membri, lo Stato membro d'origine aggiorna i dati registrati ai sensi dell'articolo 11 del presente regolamento relativi all'interessato, aggiungendo la data in cui questi ha lasciato il territorio, in modo da agevolare l'applicazione dell'articolo 19, paragrafo 2, e dell'articolo 20, paragrafo 5, del regolamento (UE) n. 604/2013;
- d) non appena si assicura che l'interessato, i cui dati sono stati registrati nell'Eurodac ai sensi dell'articolo 11 del presente regolamento, ha lasciato il territorio degli Stati membri per effetto di una decisione di rimpatrio o di un provvedimento di allontanamento emessi da quello Stato membro a seguito del ritiro o del rigetto della domanda di protezione internazionale come previsto all'articolo 19, paragrafo 3, del regolamento (UE) n. 604/2013, lo Stato membro d'origine aggiorna i dati registrati ai sensi dell'articolo 11 del presente regolamento relativi all'interessato, aggiungendo la data di allontanamento o la data in cui questi ha lasciato il territorio;
- e) lo Stato membro che diventa competente ai sensi dell'articolo 17, paragrafo 1, del regolamento (UE) n. 604/2013 aggiorna i dati registrati ai sensi dell'articolo 11 del presente regolamento relativi al richiedente protezione internazionale, aggiungendo la data in cui è stata presa la decisione di esaminare la domanda.

#### Articolo 11

##### Registrazione dei dati

Nel sistema centrale sono registrati unicamente i seguenti dati:

- a) dati relativi alle impronte digitali;
- b) Stato membro d'origine, luogo e giorno in cui è stata presentata la domanda di protezione internazionale; nei casi di cui all'articolo 10, lettera b), la data della domanda corrisponde alla data inserita dallo Stato membro che ha provveduto al trasferimento del richiedente;
- c) sesso;
- d) numero di riferimento assegnato dallo Stato membro d'origine;
- e) data di rilevamento delle impronte digitali;
- f) data della trasmissione dei dati al sistema centrale;
- g) identificativo utente dell'operatore;
- h) nei casi di cui all'articolo 10, lettera a) o b), la data di arrivo dell'interessato in seguito a trasferimento;

- i) nei casi di cui all'articolo 10, lettera c), la data in cui l'interessato ha lasciato il territorio degli Stati membri;
- j) nei casi di cui all'articolo 10, lettera d), la data in cui l'interessato ha lasciato il territorio degli Stati membri o ne è stato allontanato;
- k) nei casi di cui all'articolo 10, lettera e), la data in cui è stata presa la decisione di esaminare la domanda.

#### Articolo 12

##### Conservazione dei dati

1. Ciascuna serie di dati di cui all'articolo 11 è conservata presso il sistema centrale per dieci anni a decorrere dalla data alla quale le impronte sono state rilevate.
2. Decorso il termine di cui al paragrafo 1, i dati sono cancellati automaticamente dal sistema centrale.

#### Articolo 13

##### Cancellazione anticipata dei dati

1. I dati riguardanti le persone che hanno acquisito la cittadinanza di uno Stato membro prima della scadenza del periodo di cui all'articolo 12, paragrafo 1, sono cancellati dal sistema centrale, a norma dell'articolo 27, paragrafo 4, non appena lo Stato membro d'origine viene a conoscenza che gli interessati hanno acquisito tale cittadinanza.
2. Il sistema centrale informa, quanto prima e in ogni caso entro un periodo non superiore a 72 ore, tutti gli Stati membri d'origine della cancellazione, a cura di un altro Stato membro d'origine, dei dati ai sensi del paragrafo 1 del presente articolo che hanno generato una risposta pertinente con i dati da quelli trasmessi riguardanti persone di cui all'articolo 9, paragrafo 1, o all'articolo 14, paragrafo 1.

#### CAPO III

##### CITTADINI DI PAESI TERZI O APOLIDI FERMATI IN RELAZIONE ALL'ATTRAVERSAMENTO IRREGOLARE DI UNA FRONTIERA ESTERNA

#### Articolo 14

##### Rilevamento e trasmissione di dati relativi alle impronte digitali

1. Ciascuno Stato membro procede tempestivamente al rilevamento delle impronte digitali di tutte le dita di cittadini di paesi terzi o apolidi di età non inferiore a 14 anni, che siano fermati dalle competenti autorità di controllo in relazione all'attraversamento irregolare via terra, mare o aria della propria frontiera in provenienza da un paese terzo e che non siano stati respinti o che rimangano fisicamente nel territorio degli Stati membri e che non siano in stato di custodia, reclusione o trattenimento per tutto il periodo che va dal fermo all'allontanamento sulla base di una decisione di respingimento.

2. Lo Stato membro interessato trasmette quanto prima e in ogni caso entro 72 ore dopo la data del fermo al sistema centrale i seguenti dati relativi ai cittadini di paesi terzi o apolidi di cui al paragrafo 1 non respinti:

- a) dati relativi alle impronte digitali;
- b) Stato membro d'origine, luogo e data del fermo;
- c) sesso;
- d) numero di riferimento assegnato dallo Stato membro d'origine;
- e) data di rilevamento delle impronte digitali;
- f) data della trasmissione dei dati al sistema centrale;
- g) identificativo utente dell'operatore.

3. In deroga al paragrafo 2, i dati di cui al medesimo paragrafo 2 relativi alle persone fermate ai sensi del paragrafo 1 che rimangono fisicamente nel territorio dello Stato membro ma sono in stato di custodia, reclusione o trattenimento dal momento del fermo per oltre 72 ore, sono trasmessi prima della loro liberazione.

4. L'inosservanza del termine di 72 ore di cui al paragrafo 2 del presente articolo non dispensa gli Stati membri dal rilevare e trasmettere le impronte digitali al sistema centrale. Quando lo stato dei polpastrelli non consente di effettuare un rilevamento delle impronte di qualità tale da assicurare un confronto appropriato ai sensi dell'articolo 25, lo Stato membro d'origine provvede a rilevare nuovamente le impronte digitali delle persone fermate ai sensi del paragrafo 1 del presente articolo e le ritrasmette quanto prima e in ogni caso entro 48 ore dal buon esito del rilevamento.

5. In deroga al paragrafo 1, quando non è possibile rilevare le impronte digitali della persona fermata a causa di provvedimenti che ne tutelano la salute o per motivi di salute pubblica, lo Stato membro interessato rileva e invia dette impronte digitali quanto prima e in ogni caso entro 48 ore dal momento in cui tali motivi di salute sono venuti meno.

Nel caso di gravi problemi tecnici gli Stati membri possono prorogare di ulteriori 48 ore al massimo il termine di 72 ore di cui al paragrafo 2 al fine di attuare i piani di continuità nazionali.

#### Articolo 15

##### Registrazione dei dati

1. Sono registrati nel sistema centrale i dati di cui all'articolo 14, paragrafo 2.

Fatto salvo l'articolo 8, i dati trasmessi al sistema centrale ai sensi dell'articolo 14, paragrafo 2, sono registrati unicamente ai fini del confronto con i dati relativi ai richiedenti protezione internazionale trasmessi successivamente allo stesso sistema centrale e ai fini di cui all'articolo 1, paragrafo 2.

Il sistema centrale non confronta i dati trasmessigli ai sensi dell'articolo 14, paragrafo 2, con dati già registrati nel sistema centrale né con i dati che gli vengono successivamente trasmessi ai sensi dell'articolo 14, paragrafo 2.

2. Ai fini del confronto dei dati relativi ai richiedenti protezione internazionale trasmessi successivamente al sistema centrale con i dati di cui al paragrafo 1, si applicano le procedure di cui all'articolo 9, paragrafi 3 e 5, e all'articolo 25, paragrafo 4.

#### Articolo 16

##### Conservazione dei dati

1. Ciascuna serie di dati riguardanti i cittadini di paesi terzi o gli apolidi di cui all'articolo 14, paragrafo 1, è conservata nel sistema centrale per 18 mesi a decorrere dal rilevamento delle loro impronte digitali. Decorso tale termine, tali dati sono cancellati automaticamente dal sistema centrale.

2. I dati relativi ai cittadini di paesi terzi o agli apolidi di cui all'articolo 14, paragrafo 1, sono cancellati immediatamente dal sistema centrale a norma dell'articolo 28, paragrafo 3, non appena lo Stato membro d'origine, prima che scada il termine di 18 mesi di cui al paragrafo 1 del presente articolo, viene a conoscenza di una delle seguenti circostanze:

- a) al cittadino di un paese terzo o all'apolide è stato rilasciato un titolo di soggiorno;
- b) il cittadino di un paese terzo o l'apolide ha lasciato il territorio degli Stati membri;

c) il cittadino di un paese terzo o l'apolide ha acquisito la cittadinanza di uno Stato membro.

3. Il sistema centrale informa, quanto prima e in ogni caso entro un periodo non superiore a 72 ore, tutti gli Stati membri d'origine della cancellazione, a cura di un altro Stato membro d'origine per i motivi di cui al paragrafo 2, lettera a) o b), del presente articolo, di dati che hanno generato una risposta pertinente con i dati da quelli trasmessi riguardanti persone di cui all'articolo 14, paragrafo 1.

4. Il sistema centrale informa, quanto prima e in ogni caso entro un periodo non superiore a 72 ore, tutti gli Stati membri d'origine della cancellazione, a cura di un altro Stato membro d'origine per il motivo di cui al paragrafo 2, lettera c), del presente articolo, di dati che hanno generato una risposta pertinente con i dati da quelli trasmessi riguardanti persone di cui all'articolo 9, paragrafo 1, o 14, paragrafo 1.

#### CAPO IV

### CITTADINI DI PAESI TERZI O APOLIDI SOGGIORNANTI IRREGOLARMENTE IN UNO STATO MEMBRO

#### Articolo 17

#### Confronto dei dati relativi alle impronte digitali

1. Al fine di stabilire se un cittadino di un paese terzo o un apolide soggiornante irregolarmente nel suo territorio abbia precedentemente presentato una domanda di protezione internazionale in un altro Stato membro, ciascuno Stato membro può trasmettere al sistema centrale qualsiasi dato relativo alle impronte digitali eventualmente rilevate di tale cittadino di paese terzo o apolide, purché di età non inferiore a 14 anni, insieme al numero di riferimento assegnato.

Di norma, la verifica dell'avvenuta presentazione di una domanda di protezione internazionale in un altro Stato membro ha luogo quando:

- a) il cittadino di un paese terzo o l'apolide dichiara di avere presentato una domanda di protezione internazionale, ma non indica lo Stato membro in cui l'ha presentata;
- b) il cittadino di un paese terzo o l'apolide non chiede protezione internazionale ma rifiuta di essere rimpatriato nel suo paese di origine affermando che vi si troverebbe in pericolo; oppure
- c) il cittadino di un paese terzo o l'apolide cerca di evitare l'allontanamento con altri mezzi, rifiutandosi di cooperare alla propria identificazione, in particolare non esibendo alcun documento di identità oppure esibendo documenti falsi.

2. Quando partecipano alla procedura di cui al paragrafo 1, gli Stati membri trasmettono al sistema centrale i dati relativi alle impronte di tutte le dita o almeno degli indici e, qualora queste ultime non fossero disponibili, alle impronte di tutte le altre dita dei cittadini di paesi terzi o degli apolidi di cui al paragrafo 1.

3. I dati relativi alle impronte digitali dei cittadini di paesi terzi o degli apolidi di cui al paragrafo 1 sono trasmessi al sistema centrale esclusivamente ai fini del confronto con i dati relativi alle impronte digitali dei richiedenti protezione internazionale trasmessi da altri Stati membri e già registrati nel sistema centrale.

I dati relativi alle impronte digitali di detti cittadini di paesi terzi o apolidi non sono registrati nel sistema centrale né sono confrontati con i dati trasmessi al sistema centrale ai sensi dell'articolo 14, paragrafo 2.

4. Una volta trasmessi i risultati del confronto dei dati relativi alle impronte digitali allo Stato membro d'origine, la registrazione della ricerca è conservata dal sistema centrale esclusivamente ai fini di cui all'articolo 28. Gli Stati membri o il sistema centrale non possono conservare alcuna altra registrazione della ricerca per fini diversi.

5. Ai fini del confronto dei dati relativi alle impronte digitali trasmessi a norma del presente articolo con i dati relativi alle impronte digitali dei richiedenti protezione internazionale trasmessi da altri Stati membri e già registrati presso il sistema centrale, si applicano le procedure di cui all'articolo 9, paragrafi 3 e 5, e all'articolo 25, paragrafo 4.

#### CAPO V

### BENEFICIARI DI PROTEZIONE INTERNAZIONALE

#### Articolo 18

#### Contrassegno dei dati

1. Ai fini di cui all'articolo 1, paragrafo 1, lo Stato membro d'origine che ha concesso protezione internazionale a un richiedente protezione internazionale i cui dati siano stati precedentemente registrati nel sistema centrale conformemente all'articolo 11 contrassegna a fini di contrasto i relativi dati nel rispetto dei requisiti della comunicazione elettronica con il sistema centrale definiti dall'agenzia. Il contrassegno è conservato nel sistema centrale ai sensi dell'articolo 12 ai fini della trasmissione di cui all'articolo 9, paragrafo 5. Il sistema centrale informa tutti gli Stati membri d'origine del contrassegno apposto da un altro Stato membro d'origine ai dati che hanno generato una risposta pertinente con i dati da essi trasmessi riguardanti persone di cui all'articolo 9, paragrafo 1, o 14, paragrafo 1. Detti Stati membri d'origine contrassegnano a loro volta le serie di dati corrispondenti.

2. I dati dei beneficiari di protezione internazionale conservati nel sistema centrale e contrassegnati ai sensi del paragrafo 1 del presente articolo sono resi disponibili per il confronto a fini di cui all'articolo 1, paragrafo 2, per un periodo di tre anni a decorrere dalla data in cui all'interessato è stata concessa la protezione internazionale.

In caso di risposta pertinente, il sistema centrale trasmette i dati di cui all'articolo 11, lettere da a) a k), per tutte le serie di dati corrispondenti alla risposta pertinente. Il sistema centrale non trasmette il contrassegno di cui al paragrafo 1 del presente articolo. Al termine del periodo di tre anni, il sistema centrale blocca automaticamente la trasmissione di tali dati nel caso di richieste di confronto presentate a fini di cui all'articolo 1, paragrafo 2; i dati restano invece disponibili per il confronto ai fini di cui all'articolo 1, paragrafo 1, fino al momento della loro cancellazione. I dati bloccati non sono trasmessi e, in caso di risposta pertinente, il sistema centrale comunica allo Stato membro richiedente un risultato negativo.

3. Lo Stato membro d'origine rimuove il contrassegno precedentemente apposto ai dati di un cittadino di un paese terzo o di un apolide oppure sblocca i dati precedentemente bloccati conformemente ai paragrafi 1 o 2 del presente articolo se lo status dell'interessato è revocato o è cessato, oppure se ne viene rifiutato il rinnovo ai sensi degli articoli 14 o 19 della direttiva 2011/95/UE.

#### CAPO VI

### PROCEDURA PER IL CONFRONTO E LA TRASMISSIONE DEI DATI A FINI DI CONTRASTO

#### Articolo 19

#### Procedura per il confronto dei dati relativi alle impronte digitali con i dati Eurodac

1. Ai fini di cui all'articolo 1, paragrafo 2, le autorità designate di cui agli articoli 5, paragrafo 1, e 7, paragrafo 2, possono presentare all'autorità di verifica una richiesta motivata in formato elettronico ai sensi dell'articolo 20, paragrafo 1, unitamente al numero di riferimento da loro utilizzato, affinché siano trasmessi al sistema centrale, a fini di confronto, dati relativi alle impronte digitali attraverso il punto di accesso nazionale. Ricevuta tale richiesta, l'autorità di verifica controlla se ricorrono tutte le condizioni per richiedere un confronto di cui all'articolo 20 o all'articolo 21, a seconda dei casi.

2. Se ricorrono tutte le condizioni per richiedere un confronto di cui all'articolo 20 o all'articolo 21, l'autorità di verifica trasmette la richiesta al punto di accesso nazionale che la trasmette, ai sensi dell'articolo 9, paragrafi 3 e 5, al sistema centrale per il confronto con i dati trasmessi al sistema centrale a norma degli articoli 9, paragrafo 1, e 14, paragrafo 2.

3. In casi eccezionali di urgenza ove sia necessario per prevenire un pericolo imminente associato a reati di terrorismo o ad altri reati gravi, l'autorità di verifica può trasmettere al punto

di accesso nazionale i dati relativi alle impronte digitali per un confronto immediato appena ricevuta la richiesta da un'autorità designata e verificare solo a posteriori se siano rispettate tutte le condizioni per richiedere un confronto di cui all'articolo 20 o all'articolo 21, compresa l'effettiva sussistenza di un caso eccezionale di urgenza. La verifica a posteriori ha luogo senza indebiti ritardi previo trattamento della richiesta.

4. Se con una verifica a posteriori si accerta che l'accesso ai dati Eurodac non era giustificato, tutte le autorità che hanno avuto accesso a tali dati cancellano le informazioni comunicate dall'Eurodac e ne informano l'autorità di verifica.

#### Articolo 20

#### Condizioni per l'accesso delle autorità designate all'Eurodac

1. Ai fini di cui all'articolo 1, paragrafo 2, le autorità designate possono presentare una richiesta motivata in formato elettronico per il confronto dei dati relativi alle impronte digitali con i dati conservati nel sistema centrale nei limiti delle loro competenze, soltanto se il confronto con le seguenti banche dati non ha consentito di stabilire l'identità dell'interessato:

- le banche nazionali dei dati dattiloscopici;
- i sistemi automatizzati d'identificazione dattiloscopica di tutti gli altri Stati membri ai sensi della decisione 2008/615/GAI, qualora il confronto sia tecnicamente disponibile, a meno che non sussistano fondati motivi per ritenere che un confronto con tali sistemi non consentirebbe di stabilire l'identità dell'interessato. Tali fondati motivi sono inclusi nella richiesta motivata di confronto con i dati Eurodac presentata in formato elettronico dall'autorità designata all'autorità di verifica; e
- il sistema di informazione visti, purché siano soddisfatte le condizioni per il confronto previste dalla decisione 2008/633/GAI;

e se sono soddisfatte tutte le seguenti condizioni nel loro insieme:

- a) il confronto è necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, vale a dire esiste un interesse prevalente di sicurezza pubblica tale da rendere proporzionata l'interrogazione della banca dati;
- b) il confronto è necessario in un caso specifico (vale a dire non si eseguono confronti sistematici); e

c) esistono fondati motivi per ritenere che il confronto contribuisca in misura sostanziale alla prevenzione, all'individuazione o all'investigazione di uno dei reati in questione. Tali fondati motivi ricorrono in particolare laddove sussista il sospetto fondato che l'autore presunto o effettivo oppure la vittima di un reato di terrorismo o di un altro reato grave rientri in una delle categorie contemplate dal presente regolamento.

2. Le richieste di confronto con i dati Eurodac sono limitate alla ricerca dei dati relativi alle impronte digitali.

#### Articolo 21

##### Condizioni per l'accesso di Europol all'Eurodac

1. Ai fini di cui all'articolo 1, paragrafo 2, l'autorità designata da Europol può presentare una richiesta motivata in formato elettronico per il confronto dei dati relativi alle impronte digitali con i dati conservati nel sistema centrale nei limiti del mandato di Europol ove ciò sia necessario per l'adempimento delle funzioni di Europol, soltanto se il confronto con i dati relativi alle impronte digitali conservati nei sistemi di trattamento delle informazioni tecnicamente e giuridicamente accessibili da Europol non ha consentito di stabilire l'identità dell'interessato, e se sono soddisfatte tutte le seguenti condizioni nel loro insieme:

a) il confronto è necessario per sostenere e rafforzare l'azione degli Stati membri in materia di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi che sono di competenza di Europol, ossia esiste un interesse prevalente di sicurezza pubblica tale da rendere proporzionata la ricerca della banca dati;

b) il confronto è necessario in un caso specifico (vale a dire non si eseguono confronti sistematici); e

c) esistono fondati motivi per ritenere che il confronto contribuisca in misura sostanziale alla prevenzione, all'individuazione o all'investigazione di uno dei reati in questione. Tali fondati motivi ricorrono in particolare laddove sussista il sospetto fondato che l'autore presunto o effettivo oppure la vittima di un reato di terrorismo o di un altro reato grave rientri in una delle categorie contemplate dal presente regolamento.

2. Le richieste di confronto con i dati Eurodac sono limitate al confronto dei dati relativi alle impronte digitali.

3. Il trattamento delle informazioni ottenute da Europol mediante il confronto con i dati Eurodac è soggetto all'autorizzazione dello Stato membro d'origine. Tale autorizzazione è ottenuta attraverso l'unità nazionale Europol dello Stato membro.

#### Articolo 22

##### Comunicazione tra le autorità designate, le autorità di verifica e i punti di accesso nazionali

1. Fatto salvo l'articolo 26, tutte le comunicazioni tra le autorità designate, le autorità di verifica e i punti di accesso nazionali sono sicure e avvengono per via elettronica.

2. Ai fini di cui all'articolo 1, paragrafo 2, le impronte digitali vengono digitalizzate dagli Stati membri e trasmesse nel formato dei dati indicato nell'allegato I, in modo che i dati possano essere confrontati dal sistema informatizzato per il riconoscimento delle impronte digitali.

#### CAPO VII

##### TRATTAMENTO, PROTEZIONE DEI DATI E RESPONSABILITÀ

#### Articolo 23

##### Responsabilità in materia di trattamento dei dati

1. Lo Stato membro d'origine è tenuto a garantire:

a) la liceità del rilevamento delle impronte digitali;

b) la liceità della trasmissione al sistema centrale dei dati relativi alle impronte digitali e degli altri dati di cui all'articolo 11, all'articolo 14, paragrafo 2, e all'articolo 17, paragrafo 2;

c) l'esattezza e l'attualità dei dati al momento della trasmissione al sistema centrale;

d) ferma restando la responsabilità dell'agenzia, la liceità della registrazione, della conservazione, della rettifica e della cancellazione dei dati nel sistema centrale;

e) la liceità del trattamento dei risultati del confronto dei dati relativi alle impronte digitali trasmessi dal sistema centrale.

2. A norma dell'articolo 34, lo Stato membro d'origine garantisce la sicurezza dei dati di cui al paragrafo 1 prima e durante la trasmissione al sistema centrale, nonché la sicurezza dei dati che esso riceve da quest'ultimo.

3. Lo Stato membro d'origine è responsabile dell'identificazione definitiva dei dati ai sensi dell'articolo 25, paragrafo 4.

4. L'agenzia provvede affinché il sistema centrale operi ai sensi delle disposizioni del presente regolamento. In particolare, l'agenzia:

- a) adotta le misure necessarie affinché le persone che lavorano con il sistema centrale non trattino i dati ivi registrati per scopi diversi da quelli dell'Eurodac, quali definiti all'articolo 1;
- b) adotta le misure necessarie per garantire la sicurezza del sistema centrale a norma dell'articolo 34;
- c) fatte salve le competenze del garante europeo della protezione dei dati, garantisce che solo le persone autorizzate a lavorare con il sistema centrale abbiano accesso ai dati ivi registrati.

L'agenzia comunica al Parlamento europeo e al Consiglio, nonché al garante europeo della protezione dei dati, le misure adottate ai sensi del primo comma.

#### Articolo 24

##### Trasmissione

1. Le impronte digitali vengono digitalizzate e trasmesse nel formato dei dati di cui all'allegato I. Se necessario al funzionamento efficace del sistema centrale, l'agenzia definisce i requisiti tecnici per la trasmissione del formato dei dati da parte degli Stati membri al sistema centrale e viceversa. L'agenzia assicura che i dati relativi alle impronte digitali trasmessi dagli Stati membri possano essere confrontati dal sistema informatizzato per il riconoscimento delle impronte digitali.

2. Gli Stati membri trasmettono i dati di cui all'articolo 11, all'articolo 14, paragrafo 2, e all'articolo 17, paragrafo 2, per via elettronica. I dati di cui all'articolo 11 e all'articolo 14, paragrafo 2, sono automaticamente registrati nel sistema centrale. Se necessario al funzionamento efficace del sistema centrale, l'agenzia definisce i requisiti tecnici per assicurare che i dati possano essere adeguatamente trasmessi per via elettronica dagli Stati membri al sistema centrale e viceversa.

3. Il numero di riferimento di cui all'articolo 11, lettera d), all'articolo 14, paragrafo 2, lettera d), all'articolo 17, paragrafo 1, e all'articolo 19, paragrafo 1, rende possibile l'attribuzione univoca dei dati a una persona e allo Stato membro che trasmette i dati. Esso inoltre rende possibile asserire se tali dati si riferiscono a una persona di cui agli articoli 9, paragrafo 1, 14, paragrafo 1, o 17, paragrafo 1.

4. Il numero di riferimento inizia con la lettera o le lettere di identificazione che contraddistinguono lo Stato membro che ha trasmesso i dati, conformemente alla norma di cui all'allegato I. La lettera o le lettere di identificazione sono seguite dal codice che identifica la categoria di persone o di richieste. I dati relativi alle persone di cui all'articolo 9, paragrafo 1, sono contrassegnati da "1", quelli relativi alle persone di cui all'articolo 14, paragrafo 1, da "2", quelli relativi alle persone di cui all'articolo 17, paragrafo 1, da "3", quelli relativi alle richieste di cui all'articolo 20 da "4", quelli relativi alle richieste di cui all'articolo 21 da "5" e quelli relativi alle richieste di cui all'articolo 29 da "9".

5. L'agenzia definisce le procedure tecniche necessarie affinché gli Stati membri assicurino il ricevimento di dati univoci da parte del sistema centrale.

6. Il sistema centrale conferma il più rapidamente possibile il ricevimento dei dati trasmessi. A tal fine l'agenzia definisce i requisiti tecnici necessari ad assicurare che agli Stati membri sia fornita, se richiesta, la ricevuta di conferma.

#### Articolo 25

##### Effettuazione dei confronti e trasmissione dei risultati

1. Gli Stati membri assicurano la trasmissione di dati relativi alle impronte digitali di qualità adeguata al confronto mediante il sistema informatizzato per il riconoscimento delle impronte digitali. L'agenzia definisce la qualità adeguata dei dati relativi alle impronte digitali trasmessi, se necessario ad assicurare che i risultati del confronto effettuato dal sistema centrale raggiungano un livello molto elevato di accuratezza. Il sistema centrale verifica, non appena possibile, la qualità dei dati relativi alle impronte digitali trasmessi. Qualora essi non siano idonei al confronto mediante il sistema informatizzato per il riconoscimento delle impronte digitali, il sistema centrale informa lo Stato membro interessato. Detto Stato membro trasmette dati relativi alle impronte digitali qualitativamente adeguati usando lo stesso numero di riferimento dei precedenti dati.

2. Il sistema centrale effettua i confronti seguendo l'ordine di arrivo delle richieste. Ogni richiesta è esaminata entro 24 ore. Uno Stato membro può chiedere che, per motivi di diritto interno, i confronti ritenuti particolarmente urgenti siano effettuati entro un'ora. Qualora questi tempi non possano essere rispettati a causa di circostanze che esulano dalla responsabilità dell'agenzia, il sistema centrale esamina la richiesta in via prioritaria non appena dette circostanze sono venute meno. In tali casi, se necessario ad assicurare il funzionamento efficace del sistema centrale, l'agenzia definisce i criteri per assicurare che le richieste siano esaminate in via prioritaria.

3. L'agenzia, se necessario ad assicurare il funzionamento efficace del sistema centrale, definisce le procedure operative per l'elaborazione dei dati ricevuti e per la trasmissione del risultato del confronto.

4. Il risultato del confronto è immediatamente controllato nello Stato membro ricevente da un esperto in dattiloscopia, quale definito ai sensi delle disposizioni nazionali, avente una formazione specifica per quanto concerne i tipi di confronti di impronte digitali di cui al presente regolamento. Ai fini di cui all'articolo 1, paragrafo 1, del presente regolamento, l'identificazione definitiva è effettuata dallo Stato membro d'origine in collaborazione con gli altri Stati membri interessati, a norma dell'articolo 34 del regolamento (UE) n. 604/2013.

Le informazioni pervenute dal sistema centrale riguardanti dati comunque ritenuti inattendibili sono cancellate non appena ne sia stata accertata l'inattendibilità.

5. Se l'identificazione definitiva ai sensi del paragrafo 4 rivela che il risultato del confronto ricevuto dal sistema centrale non corrisponde ai dati relativi alle impronte digitali inviati per il confronto, gli Stati membri cancellano immediatamente il risultato del confronto e comunicano questa circostanza alla Commissione e all'agenzia quanto prima e in ogni caso entro tre giorni lavorativi.

#### Articolo 26

##### **Comunicazione tra gli Stati membri e il sistema centrale**

I dati trasmessi dagli Stati membri al sistema centrale e viceversa utilizzano l'infrastruttura di comunicazione. L'agenzia, se necessario ad assicurare il funzionamento efficace del sistema centrale, definisce le procedure tecniche necessarie all'utilizzo dell'infrastruttura di comunicazione.

#### Articolo 27

##### **Accesso ai dati registrati nell'Eurodac e loro rettifica o cancellazione**

1. Lo Stato membro d'origine ha accesso ai dati da esso trasmessi che sono registrati nel sistema centrale, ai sensi del presente regolamento.

Nessuno Stato membro può consultare i dati trasmessi da un altro Stato membro né può ricevere tali dati, ad eccezione di quelli risultanti dal confronto di cui all'articolo 9, paragrafo 5.

2. Le autorità degli Stati membri che, ai sensi del paragrafo 1 del presente articolo, hanno accesso ai dati registrati nel sistema centrale sono designate da ciascuno Stato membro ai fini di cui all'articolo 1, paragrafo 1. Tale designazione indica la specifica unità competente a svolgere i compiti connessi all'applicazione del presente regolamento. Ogni Stato membro comunica senza indugio alla Commissione e all'agenzia l'elenco di dette unità e le relative modifiche. L'agenzia pubblica l'elenco consolidato

nella *Gazzetta ufficiale dell'Unione europea*. Qualora l'elenco subisca modifiche, l'agenzia pubblica online una volta all'anno un elenco consolidato aggiornato.

3. Fatte salve le cancellazioni effettuate a norma dell'articolo 12, paragrafo 2, o dell'articolo 16, paragrafo 1, soltanto lo Stato membro d'origine ha il diritto di modificare i dati che ha trasmesso al sistema centrale, rettificandoli o integrandoli, ovvero cancellandoli.

4. Se uno Stato membro o l'agenzia è in possesso di indizi dai quali risulta che dati registrati nel sistema centrale sono di fatto inesatti, ne avvisa quanto prima lo Stato membro d'origine.

Se uno Stato membro è in possesso di indizi dai quali risulta che nel sistema centrale sono stati registrati dati in violazione del presente regolamento, ne avvisa quanto prima l'agenzia, la Commissione e lo Stato membro d'origine. Quest'ultimo controlla i dati in questione e, ove necessario, li modifica o cancella senza indugio.

5. L'agenzia non trasferisce né rende disponibili alle autorità di un paese terzo i dati registrati nel sistema centrale. Tale divieto non è applicabile ai trasferimenti dei suddetti dati verso i paesi terzi cui si applica il regolamento (UE) n. 604/2013.

#### Articolo 28

##### **Conservazione delle registrazioni**

1. L'agenzia conserva le registrazioni di tutti i trattamenti dei dati avvenuti nel sistema centrale. Le registrazioni indicano lo scopo, la data e la durata dell'accesso, i dati trasmessi, i dati impiegati per l'interrogazione e il nome dell'unità che ha inserito o estratto i dati, nonché le persone responsabili.

2. Le registrazioni di cui al paragrafo 1 del presente articolo possono essere utilizzate esclusivamente per controllare, a fini di protezione dei dati, l'ammissibilità del trattamento dei dati, nonché per garantire la sicurezza dei dati ai sensi dell'articolo 34. Le registrazioni devono essere protette da adeguate misure contro l'accesso non autorizzato e sono cancellate un anno dopo la scadenza del periodo di conservazione di cui all'articolo 12, paragrafo 1, e all'articolo 16, paragrafo 1, a meno che non siano necessarie per procedure di controllo già avviate.

3. Ai fini di cui all'articolo 1, paragrafo 1, ciascuno Stato membro adotta, in relazione al proprio sistema nazionale, le misure necessarie per conseguire gli obiettivi enunciati ai paragrafi 1 e 2 del presente articolo. Ciascuno Stato membro conserva altresì le registrazioni del personale debitamente autorizzato ad inserire e ad estrarre i dati.

## Articolo 29

**Diritti dell'interessato**

1. Lo Stato membro d'origine provvede a informare la persona di cui agli articoli 9, paragrafo 1, 14, paragrafo 1, o 17, paragrafo 1, per iscritto e se necessario oralmente, in una lingua che la persona comprende o che ragionevolmente si suppone a lei comprensibile:

- a) dell'identità del responsabile del trattamento ai sensi dell'articolo 2, lettera d), della direttiva 95/46/CE ed eventualmente del suo rappresentante;
- b) dello scopo per cui i suoi dati saranno trattati nell'Eurodac, compresa una descrizione delle finalità del regolamento (UE) n. 604/2013, conformemente all'articolo 4 dello stesso, nonché una spiegazione, in forma intelligibile e con un linguaggio semplice e chiaro, del fatto che è ammesso l'accesso degli Stati membri e di Europol all'Eurodac a fini di contrasto;
- c) dei destinatari dei dati;
- d) riguardo alla persona di cui all'articolo 9, paragrafo 1, o all'articolo 14, paragrafo 1, dell'esistenza di un obbligo di rilevamento delle sue impronte digitali;
- e) del diritto di accesso ai dati che la riguardano e del diritto di chiedere che i dati inesatti che la riguardano siano rettificati o che i dati che la riguardano trattati illecitamente siano cancellati, nonché del diritto di ottenere informazioni sulle procedure da seguire per esercitare tali diritti, compresi gli estremi del responsabile del trattamento e delle autorità nazionali di controllo di cui all'articolo 30, paragrafo 1.

2. Per quanto riguarda la persona di cui all'articolo 9, paragrafo 1, o 14, paragrafo 1, le informazioni di cui al paragrafo 1 del presente articolo sono fornite all'atto del rilevamento delle sue impronte digitali.

Per quanto riguarda la persona di cui all'articolo 17, paragrafo 1, le informazioni di cui al paragrafo 1 del presente articolo sono fornite al più tardi quando i dati che la concernono sono trasmessi al sistema centrale. Questo obbligo non sussiste nei casi in cui fornire dette informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato.

Se una persona soggetta all'articoli 9, paragrafo 1, all'articolo 14, paragrafo 1, e all'articolo 17, paragrafo 1, è un minore, gli Stati membri provvedono a comunicare le informazioni in modo consono alla sua età.

3. È redatto un opuscolo comune contenente quanto meno le informazioni di cui al paragrafo 1 del presente articolo e

all'articolo 4, paragrafo 1, del regolamento (UE) n. 604/2013, secondo la procedura di cui all'articolo 44, paragrafo 2, di detto regolamento.

L'opuscolo è scritto in modo chiaro e semplice, in una lingua che la persona interessata comprende o che o che ragionevolmente si suppone a lei comprensibile.

L'opuscolo è realizzato in modo da consentire agli Stati membri di completarlo con informazioni aggiuntive specifiche per ciascuno Stato membro. Tali informazioni specifiche includono quanto meno i diritti dell'interessato, la possibilità di ricevere assistenza da parte delle autorità nazionali di controllo nonché gli estremi dell'ufficio del responsabile del trattamento e delle autorità nazionali di controllo.

4. Ai fini di cui all'articolo 1, paragrafo 1, del presente regolamento in ciascuno Stato membro gli interessati possono, secondo le leggi, i regolamenti e le procedure di tale Stato, esercitare i diritti di cui all'articolo 12 della direttiva 95/46/CE.

Gli interessati hanno il diritto di ottenere la comunicazione dei dati a essi relativi registrati nel sistema centrale e dello Stato membro che li ha trasmessi al sistema centrale, fermo restando l'obbligo di fornire altre informazioni ai sensi dell'articolo 12, lettera a), della direttiva 95/46/CE. L'accesso ai dati può essere autorizzato soltanto da uno Stato membro.

5. Ai fini di cui all'articolo 1, paragrafo 1, in ciascuno Stato membro tutti gli interessati possono chiedere che i dati di fatto inesatti siano rettificati o che i dati registrati illecitamente siano cancellati. La rettifica e la cancellazione sono effettuate senza eccessivo indugio dallo Stato membro che ha trasmesso i dati, secondo le proprie leggi, regolamenti e procedure.

6. Ai fini di cui all'articolo 1, paragrafo 1, se i diritti di rettifica e di cancellazione sono esercitati in uno Stato membro diverso da quello o da quelli che hanno trasmesso i dati, le autorità di detto Stato membro prendono contatto con le autorità dello Stato membro o degli Stati membri che hanno trasmesso i dati affinché questi verifichino l'esattezza dei dati, nonché la liceità della loro trasmissione e registrazione nel sistema centrale.

7. Ai fini di cui all'articolo 1, paragrafo 1, qualora risulti che i dati registrati nel sistema centrale sono di fatto inesatti o vi sono stati registrati illecitamente, lo Stato membro che li ha trasmessi li rettifica o li cancella a norma dell'articolo 27, paragrafo 3. Lo Stato membro conferma per iscritto agli interessati, senza eccessivo indugio, di aver adottato le opportune misure per rettificare o cancellare i dati che li riguardano.

8. Ai fini di cui all'articolo 1, paragrafo 1, ove contesti che i dati registrati nel sistema centrale sono di fatto inesatti o vi sono stati registrati illecitamente, lo Stato membro che li ha trasmessi indica per iscritto agli interessati, senza eccessivo indugio, i motivi per cui rifiuta di rettificare o cancellare i dati in questione.

Lo Stato membro fornisce agli interessati anche le informazioni relative alle azioni che possono avviare se non accettano le spiegazioni fornite. Queste comprendono le modalità per proporre ricorso o se del caso presentare denuncia dinanzi alle autorità competenti o agli organi giurisdizionali di detto Stato membro, nonché l'assistenza finanziaria o di altro tipo disponibile secondo le leggi, i regolamenti e le procedure di tale Stato membro.

9. Ogni richiesta a norma dei paragrafi 4 e 5 contiene tutti i particolari necessari per l'identificazione dell'interessato, comprese le impronte digitali. Questi dati sono utilizzati unicamente ai fini dell'esercizio dei diritti di cui ai paragrafi 4 e 5 e sono cancellati subito dopo.

10. Le autorità competenti degli Stati membri collaborano attivamente fra di loro per rendere rapidamente effettivo l'esercizio dei diritti di cui ai paragrafi 5, 6 e 7.

11. Se una persona chiede la comunicazione dei dati che la riguardano in conformità del paragrafo 4, l'autorità competente conserva una registrazione della richiesta e delle modalità della sua presentazione sotto forma di documento scritto, che mette senza indugio a disposizione delle autorità nazionali di controllo.

12. Ai fini di cui all'articolo 1, paragrafo 1, del presente regolamento, in ciascuno Stato membro l'autorità nazionale di controllo assiste l'interessato, su sua richiesta, nell'esercizio dei suoi diritti, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46/CE.

13. Ai fini di cui all'articolo 1, paragrafo 1, del presente regolamento, l'autorità nazionale di controllo dello Stato membro che ha trasmesso i dati e l'autorità nazionale di controllo dello Stato membro in cui l'interessato si trova gli prestano assistenza e, a richiesta, consulenza nell'esercizio dei suoi diritti di rettifica o di cancellazione. Le autorità nazionali di controllo dei due Stati cooperano a tal fine. Le richieste di assistenza possono essere rivolte all'autorità nazionale di controllo dello Stato membro in cui l'interessato si trova, che le trasmette all'autorità dello Stato membro che ha trasmesso i dati.

14. In ciascuno Stato membro qualsiasi persona alla quale sia stato rifiutato il diritto di accesso di cui al paragrafo 4 può proporre ricorso o, se del caso, può presentare denuncia dinanzi

alle autorità competenti o agli organi giurisdizionali di detto Stato secondo le leggi, i regolamenti e le procedure di detto Stato.

15. Chiunque può, secondo le leggi, i regolamenti e le procedure dello Stato membro che ha trasmesso i dati, proporre ricorso o, se del caso, presentare denuncia dinanzi alle autorità competenti o agli organi giurisdizionali di detto Stato in merito ai dati che lo riguardano e che sono registrati nel sistema centrale, al fine di esercitare i suoi diritti ai sensi del paragrafo 5. Alle autorità nazionali di controllo è fatto obbligo di prestare assistenza e, a richiesta, consulenza all'interessato, ai sensi del paragrafo 13, per tutto l'iter processuale.

#### Articolo 30

##### **Vigilanza dell'autorità nazionale di controllo**

1. Ai fini di cui all'articolo 1, paragrafo 1, del presente regolamento ciascuno Stato membro dispone che l'autorità o le autorità nazionali di controllo designate a norma dell'articolo 28, paragrafo 1, della direttiva 95/46/CE controllino in modo indipendente, secondo il proprio diritto interno, che il trattamento dei dati a carattere personale da parte dello Stato membro in questione, nonché la loro trasmissione al sistema centrale avvengano lecitamente e ai sensi del presente regolamento.

2. Ogni Stato membro garantisce che la rispettiva autorità nazionale di controllo possa avvalersi della consulenza di persone in possesso di adeguate conoscenze in materia di dati relativi alle impronte digitali.

#### Articolo 31

##### **Vigilanza del garante europeo della protezione dei dati**

1. Il garante europeo della protezione dei dati controlla che tutte le attività di trattamento dei dati personali relative all'Eurodac, in particolare da parte dell'agenzia, siano effettuate ai sensi del regolamento (CE) n. 45/2001 e del presente regolamento.

2. Il garante europeo della protezione dei dati provvede affinché almeno ogni tre anni sia svolto un controllo delle attività di trattamento dei dati personali effettuate dall'agenzia, conformemente alle norme di revisione contabile internazionali. Una relazione su tale controllo è trasmessa al Parlamento europeo, al Consiglio, alla Commissione, all'agenzia e alle autorità nazionali di controllo. All'agenzia è data la possibilità di presentare osservazioni prima dell'adozione della relazione.

#### Articolo 32

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

1. Le autorità nazionali di controllo e il garante europeo della protezione dei dati, ciascuno nei limiti delle proprie competenze, cooperano attivamente nell'ambito delle rispettive responsabilità e assicurano la vigilanza coordinata dell'Eurodac.

2. Gli Stati membri provvedono affinché, ai sensi dell'articolo 33, paragrafo 2, ogni anno un organo indipendente svolga un controllo del trattamento dei dati personali a fini di cui all'articolo 1, paragrafo 2, inclusa l'analisi di un campione di richieste motivate in formato elettronico.

Il controllo è accluso alla relazione annuale degli Stati membri di cui all'articolo 40, paragrafo 7.

3. Le autorità nazionali di controllo e il garante europeo della protezione dei dati, se necessario, ciascuno nei limiti delle proprie competenze, si scambiano informazioni pertinenti, si assistono vicendevolmente nello svolgimento di revisioni e ispezioni, esaminano difficoltà di interpretazione o applicazione del presente regolamento, studiano problemi inerenti all'esercizio di una vigilanza indipendente o all'esercizio dei diritti delle persone cui i dati si riferiscono, elaborano proposte armonizzate per soluzioni congiunte di eventuali problemi e promuovono la sensibilizzazione del pubblico in materia di diritti di protezione dei dati, se necessario.

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

### Articolo 33

#### Protezione dei dati personali a fini di contrasto

1. Ciascuno Stato membro provvede affinché le disposizioni adottate a norma del diritto nazionale in applicazione della decisione quadro 2008/977/GAI siano altresì applicabili al trattamento dei dati personali effettuato dalle proprie autorità nazionali a fini di cui all'articolo 1, paragrafo 2, del presente regolamento.

2. Le autorità nazionali di controllo designate a norma della decisione quadro 2008/977/GAI controllano la liceità del trattamento dei dati personali effettuato ai sensi del presente regolamento dagli Stati membri ai fini di cui all'articolo 1, paragrafo 2, del presente regolamento, nonché la trasmissione di tali dati all'Eurodac e dall'Eurodac.

3. Il trattamento dei dati personali da parte di Europol ai sensi del presente regolamento è effettuato conformemente alla decisione 2009/371/GAI ed è sottoposto al controllo di un garante della protezione dei dati esterno e indipendente. Al trattamento dei dati personali da parte di Europol a norma del presente regolamento si applicano pertanto gli articoli 30, 31 e 32 di detta decisione. Il garante della protezione dei dati esterno e indipendente assicura che i diritti della persona non siano violati.

4. I dati personali ottenuti ai sensi del presente regolamento dall'Eurodac ai fini di cui all'articolo 1, paragrafo 2, sono trattati

soltanto a fini di prevenzione, accertamento o indagine nel quadro del caso specifico in relazione al quale i dati sono stati richiesti da uno Stato membro o da Europol.

5. Il sistema centrale, le autorità designate e di verifica ed Europol conservano la registrazione relativa alle ricerche onde permettere alle autorità nazionali di protezione dei dati e al garante europeo della protezione dei dati di verificare la conformità del trattamento dei dati alle norme dell'Unione in materia di protezione dei dati, in particolare al fine di conservare registrazioni che permettano di preparare le relazioni annuali di cui all'articolo 40, paragrafo 7. Qualora l'obiettivo sia diverso da tali fini, i dati personali e la registrazione relativa alla ricerca sono cancellati da tutti gli archivi nazionali e da quelli di Europol dopo un mese, salvo se necessari ai fini di specifiche indagini penali per le quali i dati sono stati richiesti da quello Stato membro o da Europol.

### Articolo 34

#### Sicurezza dei dati

1. Lo Stato membro d'origine garantisce la sicurezza dei dati prima e nel corso della trasmissione al sistema centrale.

2. Ciascuno Stato membro, in relazione a tutti i dati trattati dalle proprie autorità competenti a norma del presente regolamento, adotta le misure necessarie, compreso un piano di sicurezza, al fine di:

- a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani di emergenza per la protezione delle infrastrutture critiche;
- b) negare alle persone non autorizzate l'accesso alle strutture nazionali nelle quali lo Stato membro effettua operazioni ai fini dell'Eurodac (controlli all'ingresso delle strutture);
- c) impedire che supporti di dati possano essere letti, copiati, modificati o cancellati senza autorizzazione (controllo dei supporti di dati);
- d) impedire che siano inseriti dati senza autorizzazione e che sia presa visione, senza autorizzazione, di dati personali memorizzati o che essi siano modificati o cancellati senza autorizzazione (controllo della conservazione);
- e) impedire che i dati siano trattati nell'Eurodac senza autorizzazione e che i dati trattati nell'Eurodac siano modificati o cancellati senza autorizzazione (controllo dell'inserimento dei dati);
- f) garantire che le persone autorizzate ad accedere all'Eurodac abbiano accesso soltanto ai dati previsti dalla loro autorizzazione di accesso, ricorrendo all'identificativo utente individuale e unico e utilizzando esclusivamente modalità di accesso riservato (controllo dell'accesso ai dati);

- g) garantire che tutte le autorità con diritto di accesso all'Eurodac creino profili che descrivano le funzioni e le responsabilità delle persone autorizzate ad accedere ai dati e ad inserire, aggiornare, cancellare e consultare i dati, e mettano senza indugio tali profili, come pure ogni altra informazione pertinente che dette autorità possano richiedere a fini di controllo, a disposizione delle autorità nazionali di controllo di cui all'articolo 28 della direttiva 95/46/CE e all'articolo 25 della decisione quadro 2008/977/GAI, su richiesta di queste ultime (profili personali);
- h) garantire la possibilità di verificare e stabilire a quali organismi possano essere trasmessi dati personali mediante apparecchiature di comunicazione dei dati (controllo della comunicazione);
- i) garantire che sia possibile verificare e stabilire quali dati siano stati trattati nell'Eurodac, quando, da chi e per quale scopo (controllo della registrazione dei dati);
- j) impedire, in particolare mediante tecniche appropriate di cifratura, che all'atto della trasmissione di dati personali dall'Eurodac o verso l'Eurodac, oppure durante il trasporto dei supporti di dati, tali dati personali possano essere letti, copiati, modificati o cancellati senza autorizzazione (controllo del trasporto);
- k) controllare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure di carattere organizzativo relative al controllo interno per garantire l'osservanza del presente regolamento (autocontrollo) e per individuare automaticamente entro 24 ore qualsiasi evento pertinente si verifichi nell'applicazione delle misure di cui alle lettere da b) a j) che possa indicare il verificarsi di un incidente di sicurezza.

3. Gli Stati membri informano l'agenzia degli incidenti di sicurezza rilevati nei propri sistemi. L'agenzia informa gli Stati membri, Europol e il garante europeo della protezione dei dati su incidenti di sicurezza. Gli Stati membri interessati, l'agenzia ed Europol collaborano in caso di tali incidenti.

4. L'agenzia adotta le misure necessarie per conseguire gli obiettivi enunciati al paragrafo 2 per quanto riguarda il funzionamento dell'Eurodac, compresa l'adozione di un piano di sicurezza.

#### Articolo 35

#### **Divieto di trasferire dati a paesi terzi, organizzazioni internazionali o soggetti di diritto privato**

1. I dati personali provenienti dal sistema centrale, trasmessi a uno Stato membro o ad Europol ai sensi del presente

regolamento, non sono trasferiti a paesi terzi, organizzazioni internazionali o soggetti di diritto privato stabiliti all'interno o all'esterno dell'Unione, né sono messi a loro disposizione. Questo divieto si applica altresì al trattamento ulteriore di tali dati effettuato a livello nazionale o tra Stati membri ai sensi dell'articolo 2, lettera b), della decisione quadro 2008/977/GAI.

2. I dati personali provenienti da uno Stato membro e scambiati tra Stati membri in seguito a una risposta pertinente ottenuta a fini di cui all'articolo 1, paragrafo 2, non sono trasferiti a paesi terzi se sussiste un grave rischio che, a causa di tale trasferimento, l'interessato sia sottoposto a torture, pene o trattamenti disumani o degradanti o qualsiasi altra violazione dei diritti fondamentali.

3. I divieti di cui ai paragrafi 1 e 2 non pregiudicano il diritto degli Stati membri di trasferire tali dati a paesi terzi cui si applica il regolamento (UE) n. 604/2013.

#### Articolo 36

#### **Registrazione e documentazione**

1. Gli Stati membri ed Europol provvedono affinché tutte le operazioni di trattamento dei dati derivanti dalle richieste di confronto con i dati Eurodac a fini di cui all'articolo 1, paragrafo 2, siano registrate o documentate per verificare l'ammissibilità della richiesta, per controllare la liceità del trattamento dei dati, l'integrità e la sicurezza dei dati, e ai fini dell'autocontrollo.

2. Il registro o la documentazione indicano in ogni caso:

- a) lo scopo esatto della richiesta di confronto, compresa la forma di reato di terrorismo o altro reato grave in questione e, per Europol, lo scopo esatto della richiesta di confronto;
- b) i fondati motivi adottati per giustificare, conformemente all'articolo 20, paragrafo 1, del presente regolamento, il mancato confronto con altri Stati membri di cui alla decisione 2008/615/GAI;
- c) il riferimento del fascicolo nazionale;
- d) la data e l'ora esatta della richiesta di confronto inviata al sistema centrale dal punto di accesso nazionale;
- e) l'autorità che ha chiesto l'accesso per il confronto e il responsabile che ha presentato la richiesta ed elaborato i dati;

f) se è stata esperita la procedura d'urgenza di cui all'articolo 19, paragrafo 3, e la decisione presa in merito alla verifica a posteriori;

g) i dati usati per il confronto;

h) conformemente alle disposizioni nazionali o alla decisione 2009/371/GAI, l'identificazione del funzionario che ha effettuato la consultazione e del funzionario che ha ordinato di consultare i dati o di fornirli.

3. Le registrazioni e i documenti sono usati solo ai fini del controllo della liceità del trattamento dei dati e per garantire l'integrità e la sicurezza dei dati. Soltanto le registrazioni che non contengono dati personali possono essere usate ai fini del controllo e della valutazione di cui all'articolo 40. Le autorità nazionali di controllo competenti a verificare l'ammissibilità della richiesta e controllare la liceità del trattamento dei dati, l'integrità e la sicurezza dei dati, hanno accesso a tali registrazioni, su loro richiesta, per l'adempimento delle loro funzioni.

#### Articolo 37

##### Risarcimento dei danni

1. Le persone e gli Stati membri che hanno subito un danno in conseguenza di un trattamento illecito di dati o di qualsiasi altro atto incompatibile con il presente regolamento hanno diritto di ottenere un risarcimento dallo Stato membro responsabile del pregiudizio. Lo Stato membro è esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile.

2. Ogni Stato membro è responsabile per i danni causati al sistema centrale in caso di inosservanza da parte sua degli obblighi derivanti dal presente regolamento, tranne nel caso e nei limiti in cui l'agenzia o un altro Stato membro abbia omesso di adottare misure ragionevolmente idonee ad evitare i danni o a minimizzarne gli effetti.

3. Le azioni proposte contro uno Stato membro per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono disciplinate dalle leggi dello Stato membro convenuto.

#### CAPO VIII

##### MODIFICHE AL REGOLAMENTO (UE) N. 1077/2011

#### Articolo 38

##### Modifiche del regolamento (UE) n. 1077/2011

Il regolamento (UE) n. 1077/2011 è così modificato:

1) l'articolo 5 è sostituito dal seguente:

"Articolo 5

*Compiti relativi a Eurodac*

Con riguardo a Eurodac, l'agenzia svolge:

a) i compiti attribuiti all'agenzia conformemente al 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 Euro-pol a fini di contrasto (\*); e

b) i compiti relativi alla formazione sull'uso tecnico di Eurodac.

(\*) GU L 180 del 29.6.2013, pag. 1."

2) l'articolo 12, paragrafo 1, è così modificato:

a) le lettere u) e v) sono sostituite dalle seguenti:

"u) adotta la relazione annuale sulle attività del sistema centrale di Eurodac conformemente all'articolo 40, paragrafo 1, del regolamento (UE) n. 603/2013;

v) presenta osservazioni sulle relazioni del garante europeo della protezione dei dati relative ai controlli di cui all'articolo 45, paragrafo 2, del regolamento (CE) n. 1987/2006, all'articolo 42, paragrafo 2, del regolamento (CE) n. 767/2008 e all'articolo 31, paragrafo 2, del regolamento (UE) n. 603/2013 e assicura adeguato seguito a tali controlli";

b) la lettera x) è sostituita dalla seguente:

"x) elabora statistiche sulle attività del sistema centrale di Eurodac conformemente all'articolo 8, paragrafo 2, del regolamento (UE) n. 603/2013";

c) la lettera z) è sostituita dalla seguente:

"z) provvede alla pubblicazione annuale dell'elenco delle unità conformemente all'articolo 27, paragrafo 2, del regolamento (UE) n. 603/2013";

3) all'articolo 15, 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. Europol può assistere alle riunioni del consiglio di amministrazione in qualità di osservatore anche quando sono all'ordine del giorno questioni concernenti il VIS, in relazione all'applicazione della decisione 2008/633/GAI, o questioni concernenti Eurodac, in relazione all'applicazione del regolamento (UE) n. 603/2013";

4) l'articolo 17 è così modificato:

a) al paragrafo 5, la lettera g) è sostituita dalla seguente:

"g) fatto salvo l'articolo 17 dello statuto, stabilisce le clausole di riservatezza per conformarsi, rispettivamente, all'articolo 17 del regolamento (CE) n. 1987/2006, dell'articolo 17 della decisione 2007/533/GAI, all'articolo 26, paragrafo 9, del regolamento (CE) n. 767/2008 e all'articolo 4, paragrafo 4, del regolamento (UE) n. 603/2013";

b) al paragrafo 6, la lettera i) è sostituita dalla seguente:

"i) relazioni sul funzionamento tecnico di ogni sistema IT su larga scala di cui all'articolo 12, paragrafo 1, lettera t), e la relazione annuale sulle attività del sistema centrale di Eurodac di cui all'articolo 12, paragrafo 1, lettera u), sulla base dei risultati del controllo e della valutazione.";

5) all'articolo 19, il paragrafo 3 è sostituito dal seguente:

"3. Sia Europol che Eurojust possono nominare un rappresentante in seno al gruppo consultivo SIS II. Europol può nominare anche un rappresentante in seno ai gruppi consultivi VIS ed Eurodac.".

## CAPO IX

### DISPOSIZIONI FINALI

#### Articolo 39

#### Spese

1. Le spese connesse all'istituzione e alla gestione del sistema centrale e dell'infrastruttura di comunicazione sono a carico del bilancio generale dell'Unione europea.

2. Le spese per i punti di accesso nazionali, incluse quelle per il loro collegamento con il sistema centrale, sono a carico dei singoli Stati membri.

3. Gli Stati membri ed Europol istituiscono e mantengono a loro spese l'infrastruttura tecnica necessaria all'attuazione del presente regolamento e si fanno carico degli oneri derivanti dalle richieste di confronto con i dati Eurodac a fini di cui all'articolo 1, paragrafo 2.

#### Articolo 40

#### Relazione annuale, monitoraggio e valutazione

1. L'agenzia trasmette annualmente al Parlamento europeo, al Consiglio, alla Commissione e al garante europeo della protezione dei dati una relazione sull'attività del sistema centrale, nella quale esamina tra l'altro il suo funzionamento tecnico e la sua sicurezza. La relazione annuale contiene anche informazioni sulla gestione e le prestazioni dell'Eurodac, misurate sulla base di indicatori quantitativi predeterminati per gli obiettivi di cui al paragrafo 2.

2. L'agenzia provvede affinché vengano attivate procedure atte a monitorare il funzionamento del sistema centrale in rapporto a determinati obiettivi di produzione, economicità e qualità del servizio.

3. Ai fini della manutenzione tecnica, delle relazioni e delle statistiche, l'agenzia ha accesso alle informazioni necessarie riguardanti i trattamenti effettuati nel sistema centrale.

4. Entro 20 luglio 2018, e successivamente ogni quattro anni, la Commissione presenta una valutazione complessiva dell'Eurodac, nella quale analizza i risultati conseguiti rispetto agli obiettivi e l'impatto sui diritti fondamentali, onde stabilire, fra l'altro, se l'accesso a fini di contrasto provochi una discriminazione indiretta delle persone contemplate dal presente regolamento, valuta se continuano a sussistere i motivi che ne avevano giustificato l'istituzione e studia le eventuali implicazioni per la sua futura attività, formulando, se del caso, le raccomandazioni necessarie. La Commissione trasmette la valutazione al Parlamento europeo e al Consiglio.

5. Gli Stati membri forniscono all'agenzia e alla Commissione le informazioni necessarie per redigere le relazioni annuali di cui al paragrafo 1.

6. L'agenzia, gli Stati membri ed Europol forniscono alla Commissione le informazioni necessarie per redigere le relazioni di valutazione di cui al paragrafo 4. Tali informazioni non mettono a repentaglio i metodi di lavoro o non comprendono indicazioni sulle fonti, sui membri del personale o sulle indagini delle autorità designate.

7. Nel rispetto delle disposizioni del diritto nazionale relative alla pubblicazione di informazioni sensibili, gli Stati membri ed Europol predispongono ciascuno una relazione annuale sull'efficacia del confronto dei dati relativi alle impronte digitali con i dati Eurodac a fini di contrasto, in cui figurino informazioni e statistiche su:

- la finalità precisa del confronto, compreso il tipo di reato di terrorismo o altro reato grave,
- i motivi di ragionevole sospetto,
- i ragionevoli motivi adottati per giustificare il mancato confronto con altri Stati membri di cui alla decisione 2008/615/GAI, conformemente all'articolo 20, paragrafo 1, del presente regolamento,
- il numero di richieste di confronto,
- il numero e il tipo di casi in cui si è giunti a un'identificazione, e
- la necessità di trattare casi eccezionali d'urgenza, compresi i casi in cui l'autorità di verifica non ha confermato l'urgenza dopo la verifica a posteriori.

Le relazioni annuali degli Stati membri e di Europol sono trasmesse alla Commissione entro il 30 giugno dell'anno successivo.

8. Sulla base delle relazioni degli Stati membri e di Europol di cui al paragrafo 7 e oltre alla valutazione complessiva di cui al paragrafo 4, la Commissione predispone una relazione annuale sull'accesso all'Eurodac a fini di contrasto e la trasmette al Parlamento europeo, al Consiglio e al garante europeo della protezione dei dati.

#### Articolo 41

##### **Sanzioni**

Gli Stati membri adottano le misure necessarie per garantire che ogni trattamento dei dati inseriti nel sistema centrale contrario

ai fini dell'Eurodac quali definiti all'articolo 1 sia passibile di sanzioni, anche a carattere amministrativo e/o penale in conformità della legislazione nazionale, che siano effettive, proporzionate e dissuasive.

#### Articolo 42

##### **Applicazione territoriale**

Le disposizioni del presente regolamento non si applicano ai territori a cui non si applica il regolamento (UE) n. 604/2013.

#### Articolo 43

##### **Notifica delle autorità designate e delle autorità di verifica**

1. Entro 20 ottobre 2013 gli Stati membri notificano alla Commissione le autorità designate, le unità operative di cui all'articolo 5, paragrafo 3, e la sua autorità di verifica e notificano senza indugio le eventuali modifiche.

2. Entro 20 ottobre 2013 Europol notifica alla Commissione la sua autorità designata, la sua autorità di verifica e il punto di accesso nazionale designato e notifica senza indugio le eventuali modifiche.

3. La Commissione pubblica annualmente le informazioni di cui ai paragrafi 1 e 2 nella *Gazzetta ufficiale dell'Unione europea* e attraverso una pubblicazione elettronica è disponibile online e tempestivamente aggiornata.

#### Articolo 44

##### **Disposizione transitoria**

I dati bloccati nel sistema centrale ai sensi dell'articolo 12 del regolamento (CE) n. 2725/2000 sono sbloccati e contrassegnati ai sensi dell'articolo 18, paragrafo 1, del presente regolamento al 20 luglio 2015.

#### Articolo 45

##### **Abrogazione**

Il regolamento (CE) n. 2725/2000 e il regolamento (CE) n. 407/2002 sono abrogati con effetto dal 20 luglio 2015.

I riferimenti ai regolamenti abrogati vanno intesi come riferimenti al presente regolamento e letti secondo la tavola di corrispondenza di cui all'allegato III.

*Articolo 46***Entrata in vigore e decorrenza dell'applicazione**

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

Il presente regolamento si applica a decorrere da 20 luglio 2015.

Gli Stati membri notificano alla Commissione e all'agenzia di aver espletato i preparativi tecnici necessari per trasmettere i dati al sistema centrale, quanto prima e in ogni caso non oltre 20 luglio 2015.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri conformemente ai trattati.

Fatto a Bruxelles, il 26 giugno 2013

*Per il Parlamento europeo*

*Il presidente*

M. SCHULZ

*Per il Consiglio*

*Il presidente*

A. SHATTER

---

*ALLEGATO I***Formato dei dati e modulo per le impronte digitali**

Formato per lo scambio dei dati relativi alle impronte digitali

È stabilito il seguente formato per lo scambio di dati relativi alle impronte digitali:

ANSI/NIST-ITL 1a-1997, Ver.3, giugno 2001 (INT-1) e qualsiasi altro futuro sviluppo di questo standard.

Norma per le lettere che contraddistinguono lo Stato membro

Si applica la seguente norma ISO: ISO 3166 – codice di 2 lettere.

# Eurodac – Modulo per le impronte digitali

1.	Numero di riferimento	
2.	Luogo di presentazione della domanda di protezione internazionale o luogo in cui il cittadino di un paese terzo o l'apolide è stato fermato	
3.	Data di presentazione della domanda di protezione internazionale o data alla quale il cittadino di un paese terzo o l'apolide è stato fermato	
4.	Sesso	
5.	Data alla quale sono state rilevate le impronte digitali	
6.	Data alla quale i dati sono stati trasmessi al sistema centrale	

105 mm dal margine superiore del modulo  
 105 mm dal margine superiore del modulo  
 205 mm dal margine superiore del modulo

## IMPRONTE ASSUNTE PER ROTAZIONE

1. Pollice destro	2. Indice destro	3. Medio destro	4. Anulare destro	5. Mignolo destro
50 mm	40 mm	40 mm	40 mm	40 mm
40 mm				
6. Pollice sinistro	7. Indice sinistro	8. Medio sinistro	9. Anulare sinistro	10. Mignolo sinistro
40 mm				

## IMPRONTE ASSUNTE PER SOVRAPPOSIZIONE

75 mm	DUE POLLICI impronte assunte simultaneamente		75 mm
	SINISTRO	DESTRO	
	30 mm	30 mm	
65 mm	65 mm		
MANO SINISTRA Quattro dita rilevate simultaneamente		MANO DESTRA Quattro dita rilevate simultaneamente	

*ALLEGATO II***Regolamenti abrogati (di cui all'articolo 45)**

Regolamento (CE) n. 2725/2000 del Consiglio	(GU L 316 del 15.12.2000, pag. 1)
Regolamento (CE) n. 407/2002 del Consiglio	(GU L 62 del 5.3.2002 pag. 1.)

---

## ALLEGATO III

## Tavola di concordanza

Regolamento (CE) n. 2725/2000	Il presente regolamento
Articolo 1, paragrafo 1	Articolo 1, paragrafo 1
Articolo 1, paragrafo 2, primo comma, lettere a) e b)	Articolo 3, paragrafo 1, lettera a)
Articolo 1, paragrafo 2, primo comma, lettera c)	—
Articolo 1, paragrafo 2, secondo comma	Articolo 3, paragrafo 4
Articolo 1, paragrafo 3	Articolo 1, paragrafo 3
Articolo 2, paragrafo 1, lettera a)	—
Articolo 2, paragrafo 1, lettere da b) a e)	Articolo 2, paragrafo 1, lettere da a) a d)
—	Articolo 2, paragrafo 1, lettere da e) a j)
Articolo 3, paragrafo 1	—
Articolo 3, paragrafo 2	Articolo 3, paragrafo 3
Articolo 3, paragrafo 3, lettere da a) a e)	Articolo 8, paragrafo 1, lettere da a) a e)
—	Articolo 8, paragrafo 1, lettere da f) a i)
Articolo 3, paragrafo 4	—
Articolo 4, paragrafo 1	Articolo 9, paragrafo 1, e articolo 3, paragrafo 5
Articolo 4, paragrafo 2	—
Articolo 4, paragrafo 3	Articolo 9, paragrafo 3
Articolo 4, paragrafo 4	Articolo 9, paragrafo 4
Articolo 4, paragrafo 5	Articolo 9, paragrafo 5
Articolo 4, paragrafo 6	Articolo 25, paragrafo 4
Articolo 5, paragrafo 1, lettere da a) a f)	Articolo 11, lettere da a) a f)
—	Articolo 11, lettere da g) a k)
Articolo 5, paragrafo 1, lettere g) e h)	—
Articolo 6	Articolo 12
Articolo 7	Articolo 13
Articolo 8	Articolo 14
Articolo 9	Articolo 15
Articolo 10	Articolo 16
Articolo 11, paragrafi da 1 a 3	Articolo 17, paragrafi da 1 a 3
Articolo 11, paragrafo 4	Articolo 17, paragrafo 5
Articolo 11, paragrafo 5	Articolo 17, paragrafo 4
Articolo 12	Articolo 18
Articolo 13	Articolo 23
Articolo 14	—

Regolamento (CE) n. 2725/2000	Il presente regolamento
Articolo 15	Articolo 27
Articolo 16	Articolo 28, paragrafi 1 e 2
—	Articolo 28, paragrafo 3
Articolo 17	Articolo 37
Articolo 18	Articolo 29, paragrafi 1, 2, da 4 a 10 e da 12 a 15
—	Articolo 29, paragrafi 3 e 11
Articolo 19	Articolo 30
—	Articoli da 31 a 36
Articolo 20	—
Articolo 21	Articolo 39, paragrafi 1 e 2
Articolo 22	—
Articolo 23	—
Articolo 24, paragrafi 1 e 2	Articolo 40, paragrafi 1 e 2
—	Articolo 40, paragrafi da 3 a 8
Articolo 25	Articolo 41
Articolo 26	Articolo 42
—	Articoli da 43 a 45
Articolo 27	Articolo 46

  

Regolamento (CE) n. 407/2002	Il presente regolamento
Articolo 2	Articolo 24
Articolo 3	Articolo 25, paragrafi da 1 a 3
—	Articolo 25, paragrafi 4 e 5
Articolo 4	Articolo 26
Articolo 5, paragrafo 1	Articolo 3, paragrafo 3
Allegato I	Allegato I
Allegato II	—