COMMISSIONE
EUROPEA

Strasburgo, 12.12.2017
COM(2017) 794 final

2017/0352 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (cooperazione giudiziaria e di polizia, asilo e migrazione)

{SWD(2017) 473} - {SWD(2017) 474}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivazione della proposta

Negli ultimi tre anni si è assistito ad un aumento degli attraversamenti irregolari delle frontiere verso l'UE e all'evolversi delle minacce alle quali è costantemente esposta la sicurezza interna, come dimostrato dagli attentati terroristici che si sono verificati. I cittadini dell'UE si aspettano che i controlli sulle persone alle frontiere esterne e le verifiche all'interno dello spazio Schengen siano efficaci, consentendo in tal modo una gestione efficiente della migrazione e contribuendo alla sicurezza interna. Queste sfide hanno messo in maggior evidenza l'urgente necessità di collegare e rafforzare, nel loro insieme, gli strumenti di informazione dell'UE per la gestione delle frontiere, la migrazione e la sicurezza.

La gestione delle informazioni nell'UE può e deve essere resa più efficace ed efficiente, nel pieno rispetto dei diritti fondamentali tra cui, in particolare, il diritto alla protezione dei dati personali, al fine di proteggere meglio le frontiere esterne dell'UE, migliorare la gestione della migrazione e aumentare la sicurezza interna, a vantaggio di tutti i cittadini. Per fornire alle guardie di frontiera, agli operatori dei servizi dell'immigrazione e alle autorità di contrasto informazioni pertinenti riguardanti le persone esistono già diversi sistemi di informazione a livello dell'UE e altri sono in fase di sviluppo. Affinché questo sostegno sia efficace è necessario che le informazioni fornite dai sistemi di informazione dell'UE siano complete, precise e attendibili. L'architettura UE di gestione delle informazioni presenta tuttavia alcune carenze strutturali e le autorità nazionali si trovano ad operare con un panorama complesso di sistemi di informazione gestiti in maniera diversa. L'architettura della gestione dei dati per il controllo delle frontiere e la sicurezza è inoltre disorganica, poiché le informazioni sono archiviate separatamente in sistemi non interconnessi, con conseguenti zone d'ombra. **Attualmente**, perciò, **i vari sistemi di informazione a livello dell'UE non sono interoperabili**, in altre parole non sono in grado di scambiare dati e di condividere informazioni così da rendere disponibili le informazioni necessarie alle autorità e agli operatori competenti, quando e dove ne hanno bisogno. L'interoperabilità dei sistemi di informazione a livello dell'UE può contribuire in modo significativo ad eliminare le attuali zone d'ombra che rendono possibile la registrazione di persone, anche coinvolte in attività terroristiche, con nomi diversi in banche dati diverse non collegate tra loro.

Nell'aprile 2016 la Commissione ha presentato una **comunicazione dal titolo *Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza***[1] allo scopo di risolvere una serie di carenze strutturali connesse ai sistemi di informazione[2]. L'intento era quello di avviare un dibattito sul modo in cui i sistemi di informazione, nell'Unione europea potevano rafforzare la gestione delle frontiere e della migrazione e la sicurezza interna. Analogamente, riconoscendo l'urgente necessità di un'azione in questo settore, il **Consiglio**, nel giugno 2016, ha approvato una **tabella di marcia per rafforzare lo scambio e la gestione di**

[1] COM(2016) 205 del 6 aprile 2016. .

[2] 1) Funzionalità non ottimali di alcuni sistemi di informazione esistenti, 2) lacune relative alle informazioni nell'architettura della gestione dei dati dell'UE, 3) complessità dovuta all'esistenza di sistemi di informazione gestiti in maniera diversa e 4) frammentarietà dell'architettura della gestione dei dati per il controllo delle frontiere e la sicurezza, in cui le informazioni sono archiviate separatamente in sistemi non interconnessi, con conseguenti zone d'ombra.

informazioni, comprese soluzioni di interoperabilità nel settore "Giustizia e affari interni"[3]. Scopo della tabella di marcia era sostenere le indagini operative e fornire rapidamente agli operatori in prima linea — operatori di polizia, guardie di frontiera, pubblici ministeri, operatori del servizio immigrazione e altri — informazioni complete, attuali e di alta qualità per collaborare e agire in modo efficace. Anche il **Parlamento europeo** ha sollecitato un'azione nel settore e, nella risoluzione del luglio 2016[4] sul programma di lavoro della Commissione per il 2017, ha invitato a formulare "*proposte intese a migliorare e sviluppare i sistemi di informazione esistenti, far fronte alla carenza di informazioni e progredire verso l'interoperabilità nonché [...] proposte concernenti lo scambio obbligatorio di informazioni a livello dell'UE, assicurando nel contempo le necessarie garanzie in materia di protezione dei dati*". Il discorso del presidente Juncker sullo stato dell'Unione del settembre 2016[5] e le conclusioni del Consiglio europeo del dicembre 2016[6] hanno sottolineato l'importanza di colmare le attuali carenze nella gestione dei dati e di migliorare l'interoperabilità degli attuali sistemi di informazione.

Dando seguito alla comunicazione dell'aprile 2016, nel giugno dello stesso anno la Commissione ha istituito un **gruppo di esperti ad alto livello sui sistemi di informazione e sull'interoperabilità**[7] incaricato di affrontare le questioni legate agli aspetti giuridici, tecnici e operativi del miglioramento dell'interoperabilità tra i sistemi centrali dell'UE per le frontiere e la sicurezza, inclusa la loro necessità, fattibilità tecnica e proporzionalità e le loro implicazioni in termini di protezione dei dati. Nella **relazione finale** pubblicata nel maggio 2017[8] il gruppo di esperti ad alto livello ha formulato una serie di raccomandazioni volte a rafforzare e sviluppare i sistemi di informazione dell'UE e la loro interoperabilità. L'Agenzia dell'UE per i diritti fondamentali, il garante europeo della protezione dei dati e il coordinatore antiterrorismo dell'UE hanno partecipato tutti attivamente ai lavori del gruppo di esperti. Ognuno ha presentato dichiarazioni in cui ha espresso il proprio sostegno, pur riconoscendo che le questioni di più ampia portata riguardanti i diritti fondamentali e la protezione dei dati avrebbero dovuto essere affrontate in itinere. Rappresentanti del segretariato della commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo e del segretariato generale del Consiglio hanno partecipato in qualità di osservatori. Il gruppo di esperti ha concluso che era **necessario e tecnicamente fattibile adoperarsi per giungere a soluzioni pratiche in materia di interoperabilità** e che tali soluzioni, in linea di massima, potevano offrire vantaggi operativi ed essere introdotte nel rispetto dei requisiti in materia di protezione dei dati.

Alla luce della relazione e delle raccomandazioni del gruppo di esperti, la Commissione, nella *Settima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza*[9], ha delineato un **nuovo approccio alla gestione dei dati** per le frontiere e la

---

3 Tabella di marcia per rafforzare lo scambio e la gestione di informazioni, comprese soluzioni di interoperabilità nel settore "Giustizia e affari interni" — documento del Consiglio 9368/1/16 REV 1, del 6 giugno 2016.

4 Risoluzione del Parlamento europeo del 6 luglio 2016 sulle priorità strategiche per il programma di lavoro della Commissione per il 2017 (2016/2773 (RSP).

5 Stato dell'Unione 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_it.

6 Conclusioni del Consiglio europeo del 15.12.2016, http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

7 Decisione della Commissione del 17 giugno 2016 che istituisce il gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità — 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

9 COM(2017) 261 final.

sicurezza e per la gestione della migrazione, in base al quale tutti i sistemi di informazione centralizzati dell'UE per la gestione della sicurezza, delle frontiere e della migrazione risultano interoperabili, nel pieno rispetto dei diritti fondamentali. La Commissione ha annunciato l'intenzione di proseguire i lavori per la creazione di un portale di ricerca europeo capace di interrogare simultaneamente tutti i sistemi pertinenti dell'UE nei settori della gestione della sicurezza, delle frontiere e della migrazione, eventualmente con norme più snelle per l'accesso a fini di contrasto, e di sviluppare, per tali sistemi, un servizio comune di confronto biometrico (provvisto, se del caso, di una funzione di segnalazione basata su riscontri positivi o negativi, la cosiddetta funzione "hit/no hit"[10]) e un archivio comune di dati di identità. Ha inoltre annunciato l'intenzione di presentare quanto prima una proposta legislativa sull'interoperabilità.

Nelle conclusioni del giugno 2017[11], il Consiglio europeo ha ribadito la necessità di agire e, basandosi sulle conclusioni del giugno 2017[12] del Consiglio "Giustizia e affari interni", ha invitato la Commissione ad elaborare quanto prima un progetto di normativa che traducesse le raccomandazioni formulate dal gruppo di esperti ad alto livello. La presente iniziativa risponde inoltre all'invito del Consiglio a dotarsi di un quadro globale per l'accesso a fini di contrasto alle varie banche dati nel settore della giustizia e degli affari interni, in modo da garantire una maggiore semplificazione, coerenza, efficacia e attenzione alle esigenze operative[13]. Per intensificare gli sforzi miranti a fare dell'Unione europea una società più sicura, nel pieno rispetto dei diritti fondamentali, la Commissione, nel quadro del programma di lavoro per il 2018[14], ha annunciato una proposta sull'interoperabilità dei sistemi di informazione, da presentare entro la fine del 2017.

- **Obiettivi della proposta**

Gli obiettivi generali della presente iniziativa emanano dagli obiettivi del trattato di migliorare la gestione delle frontiere esterne dello spazio Schengen e di contribuire alla sicurezza interna dell'Unione europea. Scaturiscono inoltre dalle decisioni politiche della Commissione e dalle conclusioni del Consiglio (europeo) pertinenti. Sono ulteriormente precisati nell'agenda europea sulla migrazione e nelle successive comunicazioni, tra cui "Preservare e rafforzare Schengen"[15] e "Agenda europea sulla sicurezza"[16], nonché nei lavori e nelle relazioni della Commissione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza[17].

Pur basandosi, in particolare, sulla comunicazione dell'aprile 2016 e sulle conclusioni del gruppo di esperti ad alto livello, gli obiettivi della presente proposta sono intrinsecamente connessi a quanto sopra.

---

[10] Nuovo concetto di "tutela della vita privata fin dalla progettazione" che limita l'accesso a tutti i dati, riducendolo ad una semplice notifica "hit/no hit" che segnala la presenza (o l'assenza) di dati.

[11] Conclusioni del Consiglio europeo del 22 e 23 giugno 2017.

[12] Risultati della 3546ª sessione del Consiglio "Giustizia e affari interni" dell'8 e 9 giugno 2017, 10136/17.

[13] Il Comitato dei rappresentanti permanenti del Consiglio (Coreper), dopo aver dato mandato alla presidenza del Consiglio per l'avvio dei negoziati interistituzionali sul sistema di ingressi/uscite dell'UE il 2 marzo 2017, ha approvato un progetto di dichiarazione del Consiglio in cui invitava la Commissione a proporre un quadro globale per l'accesso a fini di contrasto alle varie banche dati del settore della giustizia e degli affari interni in modo da garantire una maggiore semplificazione, coerenza, efficacia e attenzione alle esigenze operative (Resoconto sommario 7177/17, del 21.3.2017).

[14] COM(2017) 650 final.

[15] COM(2017) 570 final.

[16] COM(2015) 185 final.

[17] COM(2016) 230 final.

Nello specifico, la presente proposta mira a:

(1) far sì che gli utenti finali, in particolare le guardie di frontiera, le autorità di contrasto, gli operatori dei servizi per l'immigrazione e le autorità giudiziarie possano **accedere rapidamente e in modo continuato, sistematico e controllato** alle informazioni di cui hanno bisogno per svolgere i loro compiti,

(2) fornire una soluzione per l'**individuazione di identità multiple** collegate alla stessa serie di dati biometrici, al duplice scopo di garantire la corretta identificazione delle persone in buona fede e di **contrastare la frode di identità**,

(3) agevolare le **verifiche di identità dei cittadini di paesi terzi** presenti nel territorio di uno Stato membro da parte delle autorità di polizia e

(4) agevolare e **semplificare l'accesso delle autorità di contrasto** a sistemi di informazione estranei al settore del contrasto a livello dell'UE, ove necessario a fini di prevenzione, indagine, accertamento o perseguimento di reati gravi e di terrorismo.

Oltre a questi principali obiettivi operativi, la presente proposta contribuirà anche a:

- facilitare l'**attuazione** tecnica e operativa dei nuovi sistemi di informazione, attuali e futuri, **da parte degli Stati membri**,
- rafforzare e semplificare le **condizioni di sicurezza e di protezione dei dati** che disciplinano i rispettivi sistemi,
- migliorare e armonizzare i requisiti di **qualità dei dati** dei rispettivi sistemi.

La presente proposta, infine, comprende disposizioni per la definizione e la gestione di un formato universale dei messaggi (UMF), che funga da standard europeo per lo sviluppo dei sistemi di informazione nel settore della giustizia e degli affari interni, e per l'istituzione di un archivio centrale di relazioni e statistiche.

- **Ambito di applicazione della proposta**

Insieme alla proposta gemella presentata lo stesso giorno, la presente proposta sull'interoperabilità riguarda essenzialmente i sistemi di informazione centralizzati dell'UE per la sicurezza, le frontiere e la gestione della migrazione, di cui tre sono già funzionanti, uno sta per essere di sviluppato e altri due sono allo stadio di proposta in discussione tra i colegislatori. Ciascun sistema ha obiettivi, finalità, basi giuridiche, norme, gruppi di utenti e contesto istituzionale propri.

I tre sistemi di informazione centralizzati ad oggi funzionanti sono:

- il **sistema d'informazione Schengen (SIS)**, che prevede un ampio spettro di segnalazioni relative alle persone (rifiuto di ingresso o di soggiorno, mandato d'arresto europeo, persone scomparse, assistenza nel quadro di un procedimento

giudiziario, controllo discreto e controllo specifico) e agli oggetti (inclusi i documenti di identità o di viaggio smarriti, rubati o invalidati)[18],

- il sistema **Eurodac**, contenente dati relativi alle impronte digitali di richiedenti asilo e cittadini di paesi terzi che hanno attraversato irregolarmente le frontiere esterne o il cui soggiorno in uno Stato membro è irregolare,
- il **sistema di informazione visti (VIS)**, contenente dati sui visti per soggiorni di breve durata.

Oltre ai suddetti sistemi già funzionanti, nel 2016-2017 la Commissione ha proposto tre nuovi sistemi di informazione centralizzati a livello dell'UE:

- il **sistema di ingressi/uscite (EES)**, la cui base giuridica è stata appena concordata e che sostituirà l'attuale sistema di timbratura manuale dei passaporti, registrando elettronicamente il nome, il tipo di documento di viaggio, i dati biometrici, nonché la data e il luogo di ingresso e di uscita dei cittadini di paesi terzi che entrano nello spazio Schengen per un soggiorno di breve durata,
- il **sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)**, attualmente in fase di proposta, che, una volta adottato, sarà ampiamente automatizzato e in grado di raccogliere e verificare le informazioni fornite dai cittadini di paesi terzi esenti dal visto prima di un loro viaggio nello spazio Schengen,
- il **sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (sistema ECRIS-TCN)**, attualmente in fase di proposta, vale a dire un sistema elettronico per lo scambio di informazioni sulle condanne pronunciate da organi giurisdizionali penali all'interno dell'UE a carico di tali cittadini.

Questi sei sistemi, tra loro complementari, riguardano esclusivamente i cittadini di paesi terzi, ad eccezione del sistema d'informazione Schengen (SIS), e aiutano le autorità nazionali nella gestione delle frontiere, della migrazione, delle procedure di rilascio dei visti e dell'asilo, nonché nella lotta contro la criminalità e il terrorismo. Quest'ultima riguarda in particolare il SIS, che al momento rappresenta lo strumento più utilizzato per lo scambio di informazioni a fini di contrasto.

Oltre a questi sistemi di informazione, gestiti in modo centralizzato a livello dell'UE, l'ambito di applicazione della presente proposta include anche la banca dati **Interpol** sui documenti di viaggio rubati o smarriti (SLTD), interrogata in modo sistematico alle frontiere esterne dell'UE ai sensi delle disposizioni del codice frontiere Schengen, e la banca dati Interpol sui documenti di viaggio associati a segnalazioni (TDAWN). Copre inoltre i dati **Europol**, se pertinenti ai fini del funzionamento dell'ETIAS proposto e del supporto agli Stati membri nella ricerca di dati concernenti i reati gravi e di terrorismo.

I sistemi di informazione nazionali e i sistemi di informazione decentrati dell'UE non rientrano nell'ambito di applicazione della presente iniziativa. I sistemi decentrati quali quelli previsti dal quadro di Prüm[19], dalla direttiva sul codice di prenotazione (PNR)[20] e dalla

[18] I progetti di regolamento della Commissione del dicembre 2016 sul SIS ne propongono un ampliamento per inserirvi le decisioni di rimpatrio e i controlli di indagine.

[19] http://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1508936184412&uri=CELEX:32008D0615.

[20] http://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1508936384641&uri=CELEX:32016L0681.

direttiva riguardante le informazioni anticipate sui passeggeri[21] potranno essere collegati in un secondo tempo a una o più componenti proposte nel quadro della presente iniziativa[22], purché se ne dimostri la necessità.

Per rispettare la distinzione tra le questioni che rappresentano uno sviluppo dell'*acquis* di Schengen in materia di frontiere e visti, da un lato, e gli altri sistemi riguardanti l'*acquis* di Schengen in materia di cooperazione di polizia o non connessi all'*acquis* di Schengen, dall'altro, la presente proposta verte sull'accesso al sistema d'informazione Schengen quale attualmente disciplinato dalla decisione 2007/533/GAI del Consiglio, nonché sull'Eurodac e [sul sistema ECRIS-TCN].

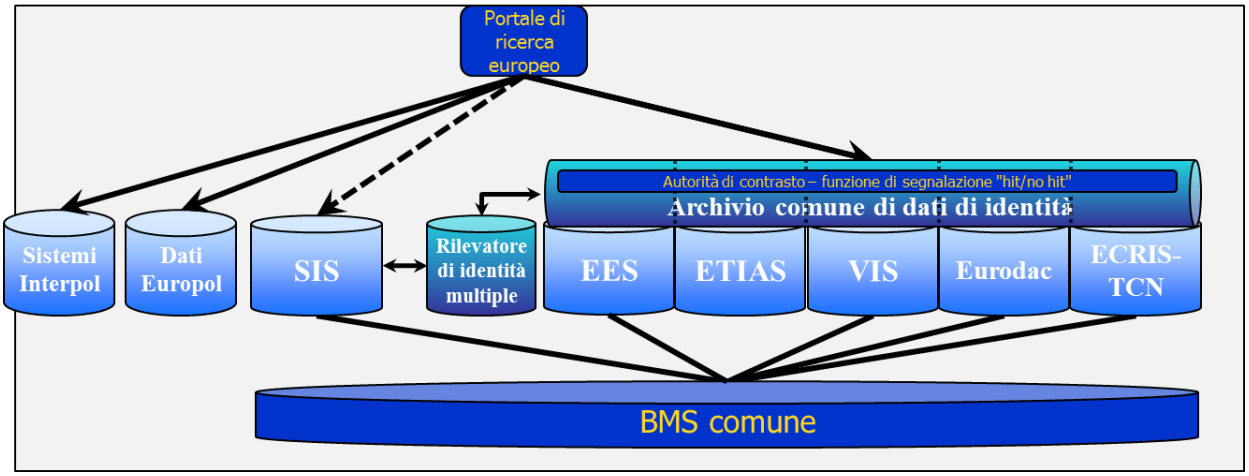
- **Componenti tecniche necessarie per realizzare l'interoperabilità**

Per conseguire gli obiettivi della presente proposta occorre istituire quattro componenti dell'interoperabilità:

- un portale di ricerca europeo (ESP),
- un servizio comune di confronto biometrico (BMS comune),
- un archivio comune di dati di identità (CIR),
- un rilevatore di identità multiple (MID).

Ciascuna di queste componenti è descritta nei dettagli nel documento di lavoro dei servizi della Commissione sulla valutazione d'impatto che accompagna la presente proposta.

Con la combinazione delle quattro componenti si configura il seguente quadro di interoperabilità:



Gli obiettivi e il funzionamento delle quattro componenti possono essere sintetizzati come segue.

[21] Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

[22] Analogamente, per quanto riguarda i sistemi doganali, nelle conclusioni del giugno 2017 il Consiglio ha invitato la Commissione ad effettuare uno studio di fattibilità che esaminasse ulteriormente gli aspetti tecnici, operativi e giuridici dell'interoperabilità dei sistemi di sicurezza e gestione delle frontiere con i sistemi doganali e a sottoporre le sue conclusioni al Consiglio a fini di discussione entro la fine del 2018.

1) Il **portale di ricerca europeo (ESP)** sarà la componente che permetterà di interrogare simultaneamente più sistemi (il SIS centrale, l'Eurodac, il VIS, il futuro EES e l'ETIAS e il sistema ECRIS-TCN proposti, nonché i sistemi Interpol e i dati Europol d'interesse) sulla base dei dati di identità (sia anagrafici che biometrici). Farà sì che gli utenti dei sistemi di informazione dell'UE possano accedere rapidamente e in modo continuato, efficace, sistematico e controllato a tutte le informazioni di cui hanno bisogno per svolgere i loro compiti.

A seguito di un'interrogazione, il portale restituirà immediatamente, nel giro di pochi secondi, informazioni provenienti dai vari sistemi ai quali l'utente ha legittimamente accesso. A seconda della finalità dell'interrogazione e dei diritti d'accesso corrispondenti, l'ESP sarà dotato di configurazioni specifiche.

L'ESP non elaborerà nuove informazioni né archivierà alcun dato; fungerà da interfaccia unica o da mediatore di messaggi (*message broker*) per interrogare vari sistemi centrali e recuperare agevolmente le informazioni necessarie, nel pieno rispetto dei requisiti concernenti il controllo degli accessi e la protezione dei dati dei sistemi sottostanti. Faciliterà l'uso corretto e autorizzato di ciascuno dei sistemi di informazione dell'UE esistenti, rendendone più semplici e meno costosi l'utilizzo e la consultazione da parte degli Stati membri, in linea con gli strumenti giuridici che li disciplinano.

2) Il **servizio comune di confronto biometrico (BMS comune)** consentirà l'interrogazione e il confronto dei dati biometrici (impronte digitali e immagini del volto) contenuti in vari sistemi centrali (in particolare, il SIS, l'Eurodac, il VIS, il futuro EES e il sistema ECRIS-TCN proposto). L'ETIAS proposto non conterrà dati biometrici e, di conseguenza, non sarà collegato al BMS comune.

Se ciascun sistema centrale esistente (SIS, Eurodac e VIS) dispone attualmente di un proprio motore di ricerca specifico per i dati biometrici[23], il servizio comune di confronto biometrico servirà da piattaforma comune in cui interrogare e confrontare simultaneamente le informazioni. Basandosi su una sola componente tecnologica al posto di cinque distinte, il BMS comune apporterà benefici considerevoli in termini di sicurezza, costi, manutenzione e funzionamento. I dati biometrici (impronte digitali e immagini del volto) saranno detenuti in via esclusiva dai sistemi sottostanti. Il BMS comune creerà e conserverà una rappresentazione matematica dei campioni biometrici (il cosiddetto "template"), ma rimuoverà i dati reali che, pertanto, rimarranno archiviati in un unico luogo, una volta sola.

Il BMS comune sarà una componente chiave che aiuterà a individuare i collegamenti tra le serie di dati e le diverse identità assunte da una stessa persona in sistemi centrali differenti. Senza di esso, nessuna delle altre tre componenti sarà in grado di funzionare.

3) L'**archivio comune di dati di identità (CIR)** sarà la componente comune in cui verranno conservati i dati di identità, sia anagrafici[24] che biometrici, dei cittadini di paesi terzi registrati nell'Eurodac, nel VIS, nel futuro EES, nonché nell'ETIAS e nel sistema ECRIS-TCN proposti. Ciascuno di questi cinque sistemi centrali registra già, o registrerà

[23] Si tratta di motori di ricerca biometrici tecnicamente conosciuti come AFIS (sistema automatico per il riconoscimento delle impronte digitali) o ABIS (sistema automatizzato di identificazione biometrica).

[24] Il documento di viaggio riporta, tra i dati anagrafici, il cognome, il nome, il sesso e la data di nascita, oltre al numero del documento. Non riporta invece gli indirizzi, i nomi precedenti, i dati biometrici, ecc.

in futuro, i dati anagrafici di determinate persone per motivi specifici, il che non è destinato a cambiare. I dati di identità pertinenti saranno conservati nel CIR, ma continueranno ad "appartenere" ai rispettivi sistemi sottostanti che li hanno registrati.

Il CIR non conterrà dati SIS: la complessa architettura tecnica del SIS contiene copie nazionali, copie nazionali parziali ed eventuali sistemi nazionali di confronto biometrico e renderebbe il CIR talmente complesso da non essere più tecnicamente né finanziariamente realizzabile.

Obiettivo principale del CIR sarà facilitare l'identificazione anagrafica di un cittadino di paese terzo. Il CIR renderà le operazioni più rapide, migliorerà l'efficienza e genererà economie di scala. Istituirlo è necessario, se si vuol far sì che le verifiche di identità dei cittadini di paesi terzi, anche nel territorio di uno Stato membro, siano efficaci. Aggiungendo al CIR un'apposita funzione di segnalazione sarà possibile verificare la presenza (o l'assenza) di dati in qualunque sistema coperto dal CIR mediante una semplice notifica "hit/no hit" (riscontro positivo/negativo). In questo modo, il CIR contribuirà anche a semplificare l'accesso delle autorità di contrasto a sistemi di informazione estranei al settore del contrasto, mantenendo nel contempo un livello elevato di protezione dei dati (cfr. punto seguente riguardante l'approccio in due fasi per l'accesso a fini di contrasto).

Dei cinque sistemi che saranno coperti dal CIR, il futuro EES e l'ETIAS e il sistema ECRIS-TCN proposti sono nuovi e ancora da sviluppare. Al momento, l'Eurodac non contiene dati anagrafici; tale estensione sarà predisposta non appena sarà stata adottata la sua nuova base giuridica. Neanche il VIS contiene attualmente dati anagrafici, ma le interazioni necessarie con il futuro EES ne richiederanno un aggiornamento in tal senso. La creazione del CIR, perciò, giungerà al momento opportuno e non implicherà in alcun modo doppioni di dati già esistenti. Dal punto di vista tecnico, il CIR sarà sviluppato sulla base della piattaforma EES/ETIAS.

4) Il **rilevatore di identità multiple (MID)** verificherà se i dati di identità oggetto dell'interrogazione sono presenti in più di uno dei sistemi ad esso collegati. Il MID coprirà i sistemi che conservano i dati di identità agganciati al CIR (l'Eurodac, il VIS, il futuro EES e l'ETIAS e il sistema ECRIS-TCN proposti) e il SIS e permetterà di individuare identità multiple collegate alla stessa serie di dati biometrici, al duplice scopo di garantire la corretta identificazione delle persone in buona fede e di contrastare la frode di identità.

Il MID consentirà di stabilire se nomi diversi corrispondono a una stessa identità. Si tratta di un'innovazione necessaria per contrastare in modo efficace l'uso fraudolento delle identità, che rappresenta una grave violazione della sicurezza. Il MID si limiterà ad evidenziare le registrazioni di identità anagrafica per le quali esiste un collegamento in sistemi centrali diversi. Il collegamento sarà rilevato utilizzando il servizio comune di confronto biometrico sulla base di dati biometrici e dovrà essere confermato o confutato dall'autorità che ha registrato nel sistema di informazione i dati all'origine del collegamento stesso. Per assistere gli utenti autorizzati del MID in questo compito, il sistema dovrà etichettare i collegamenti individuati suddividendoli in quattro categorie:

- collegamento giallo: potenziale presenza di identità anagrafiche diverse per la stessa persona;

- collegamento bianco: conferma che le diverse identità anagrafiche si riferiscono alla stessa persona in buona fede;
- collegamento verde: conferma che diverse persone in buona fede hanno la stessa identità anagrafica;
- collegamento rosso: sospetto che la stessa persona utilizzi illecitamente identità anagrafiche diverse.

La presente proposta descrive le procedure da mettere in atto per gestire queste diverse categorie. Qualunque ambiguità relativa all'identità delle persone in buona fede dovrebbe essere fugata il più rapidamente possibile mediante la trasformazione del collegamento giallo in uno verde o bianco confermato, così da non creare inutili inconvenienti. Se la valutazione porta invece alla conferma di un collegamento rosso o alla trasformazione di un collegamento giallo in un collegamento rosso, occorrerà agire di conseguenza.

- **Approccio in due fasi per l'accesso a fini di contrasto previsto dall'archivio comune di dati di identità**

L'attività di contrasto è definita come un obiettivo secondario o accessorio dell'Eurodac, del VIS, del futuro EES e dell'ETIAS proposto. Di conseguenza, la possibilità di accedere ai dati conservati in questi sistemi a fini di contrasto è limitata. Le autorità preposte possono consultare direttamente tali sistemi di informazione, estranei al settore del contrasto, soltanto a fini di prevenzione, indagine, accertamento o perseguimento di reati di terrorismo o di altri reati gravi. I rispettivi sistemi, inoltre, prevedono attualmente condizioni di accesso e garanzie diverse, alcune delle quali potrebbero ostacolare la rapidità di un loro utilizzo legittimo da parte di tali autorità. Più in generale, il principio della ricerca preliminare limita la possibilità delle autorità degli Stati membri di consultare i sistemi per finalità di contrasto giustificate e potrebbe quindi tradursi nella mancata opportunità di rinvenire le informazioni necessarie.

Nella comunicazione dell'aprile 2016 la Commissione ha riconosciuto la necessità di ottimizzare gli strumenti esistenti a fini di contrasto, rispettando nel contempo i requisiti concernenti la protezione dei dati. Tale necessità è stata confermata e ribadita dagli Stati membri e dalle agenzie pertinenti nell'ambito del gruppo di esperti ad alto livello.

Alla luce di quanto sopra, con la creazione del CIR provvisto della cosiddetta funzione di segnalazione "hit/no hit" la presente proposta introduce la possibilità di accedere all'EES, al VIS, all'ETIAS e all'Eurodac utilizzando un **approccio in due fasi per la consultazione dei dati**. L'attività di contrasto resterà un obiettivo assolutamente accessorio di tali sistemi e, di conseguenza, dovrà sottostare a regole di accesso rigorose e su ciò il nuovo approccio non avrà alcuna incidenza.

Nella prima fase, l'operatore preposto all'attività di contrasto lancerà l'interrogazione su una certa persona utilizzando i relativi dati di identità, il relativo documento di viaggio o i relativi dati biometrici al fine di verificare se le informazioni che la riguardano sono conservate nel CIR. In caso affermativo, otterrà **una risposta che indicherà il sistema o i sistemi di informazione dell'UE contenenti dati** sull'interessato (il cosiddetto **"hit"**, o riscontro positivo). L'operatore non avrà effettivo accesso a nessun dato contenuto nei vari sistemi sottostanti.

Nella seconda fase, l'operatore potrà chiedere singolarmente l'accesso a ciascun sistema indicato come contenente i dati, allo scopo di ottenere il fascicolo completo riguardante la persona oggetto dell'interrogazione, **in linea con le norme vigenti e le procedure stabilite da ciascun sistema interessato**. Questo secondo accesso rimarrà condizionato all'autorizzazione preventiva di un'autorità designata e all'uso di uno specifico identificativo (ID) dell'utente e delle relative credenziali di accesso.

Tenuto conto dell'**esistenza di possibili collegamenti** nel MID, il nuovo approccio dovrebbe inoltre portare valore aggiunto alle autorità di contrasto. Il MID aiuterà il CIR ad individuare i collegamenti esistenti, rendendo la ricerca ancor più accurata, e sarà in grado di indicare se la persona interessata è **conosciuta con identità diverse** in sistemi di informazione diversi.

La consultazione dei dati in due fasi sarà particolarmente utile nel caso in cui l'autore presunto o effettivo oppure la vittima presunta di un reato di terrorismo o di un altro reato grave **sia sconosciuto/sconosciuta**. In questi casi, infatti, il CIR permetterà di individuare con un'unica ricerca il sistema di informazione che conosce l'interessato. Diventa in tal modo superfluo applicare le condizioni attualmente vigenti ai sensi della decisione 2008/615/GAI relativamente alle ricerche preliminari da effettuarsi nelle banche dati nazionali e ad una ricerca preventiva nel sistema automatico di identificazione dattiloscopica di altri Stati membri ("controllo a norma del trattato di Prüm").

Il nuovo approccio di consultazione in due fasi **entrerà in vigore solo dopo che le componenti** necessarie per garantire l'interoperabilità **saranno rese pienamente operative**.

- **Elementi aggiuntivi a sostegno delle componenti dell'interoperabilità**

1) In aggiunta alle suddette componenti, la presente proposta di regolamento propone anche l'istituzione di un **archivio centrale di relazioni e statistiche (CRRS)** che consenta la creazione e lo scambio di relazioni contenenti dati statistici (anonimi) a fini strategici, operativi e di qualità dei dati. L'attuale prassi di raccolta di dati statistici solo da singoli sistemi di informazione nuoce alla sicurezza dei dati e all'efficienza e non consente la correlazione dei dati tra i vari sistemi.

   Il CRRS servirà da archivio apposito e a sé stante per i dati statistici anonimi estratti dal SIS, dal VIS, dall'Eurodac, dal futuro EES, dall'ETIAS e dal sistema ECRIS-TCN proposti, dall'archivio comune di dati di identità, dal rilevatore di identità multiple e dal servizio comune di confronto biometrico. Offrirà agli Stati membri, alla Commissione (incluso Eurostat) e alle agenzie dell'UE la possibilità di scambiare relazioni in modalità protetta (secondo quanto previsto dai rispettivi strumenti giuridici).

   Lo sviluppo di un archivio centrale unico invece che di tanti archivi separati, uno per ciascun sistema, ridurrà i costi e gli sforzi necessari per l'istituzione, il funzionamento e la manutenzione. Garantirà inoltre un maggior livello di sicurezza dei dati, poiché la loro conservazione e la gestione del controllo degli accessi si limiteranno ad un unico archivio.

2) La presente proposta di regolamento propone inoltre di usare il **formato universale dei messaggi (UMF)** come standard a livello dell'UE per coordinare l'interazione di più sistemi in modo interoperabile, inclusi i sistemi sviluppati e gestiti dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e

giustizia (eu-LISA). Sarà incoraggiato l'uso del formato anche da parte di Europol e Interpol.

Lo standard UMF introdurrà un linguaggio tecnico comune e armonizzato per descrivere e collegare elementi di dati, in particolare quelli riguardanti le persone e i documenti (di viaggio). In fase di sviluppo di nuovi sistemi di informazione, l'uso dell'UMF agevola l'integrazione e l'interoperabilità con altri sistemi, in particolare per gli Stati membri che hanno bisogno di creare interfacce per comunicare con questi nuovi sistemi. In questo senso, l'uso obbligatorio dell'UMF in fase di sviluppo di nuovi sistemi può essere considerato un presupposto necessario per l'introduzione delle componenti dell'interoperabilità proposte nel presente regolamento.

Per garantire la completa diffusione dello standard UMF in tutta l'UE si propone una struttura di gestione adeguata. La Commissione sarà responsabile dell'istituzione e dello sviluppo dello standard UMF nel quadro di una procedura d'esame con gli Stati membri. Vi saranno coinvolti anche gli Stati associati Schengen, le agenzie dell'UE e gli organismi internazionali che partecipano ai progetti UMF (quali eu-LISA, Europol e Interpol). La struttura di gestione proposta è di vitale importanza per poter estendere e ampliare lo standard UMF assicurandone nel contempo la massima fruibilità e applicabilità.

3) La presente proposta di regolamento introduce anche i concetti di **meccanismi automatizzati di controllo della qualità dei dati** e di indicatori comuni di qualità, nonché la necessità per gli Stati membri di garantire il livello di qualità più elevato nell'alimentare e utilizzare i sistemi. Una qualità non ottimale dei dati può incidere negativamente non solo sulla capacità di identificare le persone ricercate, ma anche sui diritti fondamentali delle persone innocenti. Per ovviare agli eventuali problemi che potrebbero derivarne, gli errori umani all'atto dell'inserimento dei dati possono essere evitati grazie ad apposite norme di convalida automatica. L'obiettivo sarà quello di individuare automaticamente i dati inviati che sono palesemente errati o incoerenti, affinché lo Stato membro da cui provengono sia in grado di verificarli e di provvedere a tutte le misure correttive necessarie. Tutto ciò sarà completato dall'elaborazione di relazioni periodiche sulla qualità dei dati da parte di eu-LISA.

- **Conseguenze per altri strumenti giuridici**

Insieme proposta gemella, la presente proposta di regolamento introduce innovazioni che richiederanno la modifica di altri strumenti giuridici, segnatamente:

- il regolamento (UE) 2016/399 (codice frontiere Schengen),
- il regolamento (UE) 2017/2226 (regolamento EES),
- il regolamento (CE) n. 767/2008 (regolamento VIS),
- la decisione 2004/512/CE del Consiglio (decisione VIS),
- la decisione 2008/633/GAI del Consiglio (decisione relativa all'accesso al VIS a fini di contrasto),
- [il regolamento ETIAS],
- [il regolamento Eurodac],
- [i regolamenti SIS],

- [il regolamento ECRIS-TCN, comprese le corrispondenti disposizioni del regolamento (UE) 2016/1624 (regolamento relativo alla guardia costiera e di frontiera europea)],
- [il regolamento eu-LISA].

Insieme alla proposta gemella, la presente proposta include disposizioni dettagliate sulle modifiche da apportare ai seguenti strumenti giuridici, che attualmente si configurano come testi stabili adottati dai colegislatori: il codice frontiere Schengen, il regolamento EES, il regolamento VIS, la decisione 2008/633/GAI del Consiglio e la decisione 2004/512/CE del Consiglio.

Gli altri strumenti sopra elencati (regolamenti ETIAS, Eurodac, SIS, ECRIS-TCN ed eu-LISA) sono attualmente in fase di negoziazione in sede di Parlamento europeo e di Consiglio. In questa fase, pertanto, non è possibile definire le modifiche necessarie per tali strumenti. La Commissione le presenterà, per ciascuno di essi, entro due settimane dal raggiungimento di un accordo politico sui rispettivi progetti di regolamento.

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

La presente proposta, che si inserisce nel quadro del più ampio processo avviato con la comunicazione dell'aprile 2016 dal titolo *Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza* e dei successivi lavori del gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità, intende perseguire i tre obiettivi seguenti:

a) rafforzare e ottimizzare i benefici dei **sistemi di informazione esistenti**,

b) colmare le lacune in materia di informazioni mediante la creazione di nuovi sistemi di informazione,

c) migliorare l'interoperabilità tra questi sistemi.

Relativamente al primo obiettivo, la Commissione, nel dicembre 2016, ha adottato alcune proposte per l'ulteriore rafforzamento dell'attuale sistema d'informazione Schengen (SIS)[25]. Per quanto concerne l'Eurodac, a seguito della proposta della Commissione del maggio 2016[26], i negoziati sulla base giuridica riveduta sono stati accelerati. Attualmente è in fase di preparazione anche una proposta di nuova base giuridica per il sistema di informazione visti (VIS), che sarà presentata nel secondo trimestre del 2018.

Quanto al secondo obiettivo, i negoziati sulla proposta della Commissione dell'aprile 2016 relativa all'istituzione di un sistema di ingressi/uscite (EES)[27] si sono conclusi già nel luglio 2017 con il raggiungimento di un accordo politico tra i colegislatori, confermato dal Parlamento europeo nell'ottobre 2017 e adottato formalmente dal Consiglio nel novembre 2017. L'entrata in vigore della base giuridica è fissata per il dicembre 2017. I negoziati riguardanti la proposta del novembre 2016 di istituire un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)[28] sono cominciati e dovrebbero concludersi nei prossimi mesi. Nel giugno 2017 la Commissione ha proposto una base giuridica per colmare un'altra lacuna a livello informativo: il sistema europeo di informazione sui casellari giudiziali

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.

riguardo ai cittadini di paesi terzi (sistema ECRIS-TCN)[29]. Anche in questo caso i colegislatori hanno precisato la loro intenzione di giungere, in tempi brevi, all'adozione di tale base giuridica.

La presente proposta concerne il terzo obiettivo individuato dalla comunicazione dell'aprile 2016.

- **Coerenza con le altre normative dell'Unione nel settore della giustizia e degli affari interni**

Unitamente alla proposta gemella, la presente proposta dà seguito ed è in linea con l'agenda europea sulla migrazione e con le successive comunicazioni, tra cui quella mirante alla salvaguardia e al rafforzamento dello spazio Schengen[30], l'agenda europea sulla sicurezza[31] e i lavori e le relazioni della Commissione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza[32]. È coerente con altre politiche dell'Unione riguardanti in particolare:

- la sicurezza interna: l'agenda europea sulla sicurezza sottolinea che norme comuni rigorose riguardanti la gestione delle frontiere sono essenziali per prevenire la criminalità e il terrorismo transfrontalieri. Offrendo alle autorità i mezzi per poter accedere rapidamente e in modo continuato, sistematico e controllato alle informazioni di cui hanno bisogno, la presente proposta contribuisce ulteriormente al conseguimento di un elevato livello di sicurezza interna;
- l'asilo: la proposta include l'Eurodac tra i sistemi centrali dell'UE da rendere interoperabili;
- la gestione delle frontiere esterne e la sicurezza: la presente proposta rafforza sia i sistemi SIS e VIS, che contribuiscono ad un efficace controllo delle frontiere esterne dell'Unione, sia il futuro EES e l'ETIAS e il sistema ECRIS-TCN proposti.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

La base giuridica principale sarà costituita dalle seguenti disposizioni del trattato sul funzionamento dell'Unione europea: l'articolo 16, paragrafo 2, l'articolo 74, l'articolo 78, paragrafo 2, lettera e), l'articolo 79, paragrafo 2, lettera c), l'articolo 82, paragrafo 1, lettera d), l'articolo 85, paragrafo 1, l'articolo 87, paragrafo 2, lettera a), e l'articolo 88, paragrafo 2.

Ai sensi dell'articolo 16, paragrafo 2, l'Unione è competente ad adottare misure relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle sue istituzioni, dei suoi organi e dei suoi organismi, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e norme relative alla libera circolazione di tali dati. Ai sensi dell'articolo 74, il Consiglio può adottare misure al fine di assicurare la cooperazione amministrativa tra i servizi degli Stati membri nel settore della giustizia, della libertà e della sicurezza. Ai sensi dell'articolo 78, l'Unione è competente ad adottare misure relative a un sistema europeo

[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.
[32] COM(2016) 230 final.

comune di asilo. Ai sensi dell'articolo 79, paragrafo 2, lettera c), l'Unione è competente ad adottare misure nel settore dell'immigrazione clandestina e del soggiorno irregolare. Ai sensi dell'articolo 82, paragrafo 1, lettera d), e dell'articolo 87, paragrafo 2, lettera a), l'Unione è competente ad adottare misure volte a rafforzare la cooperazione giudiziaria e di polizia per quel che riguarda la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni. Ai sensi dell'articolo 85, paragrafo 1, e dell'articolo 88, paragrafo 2, l'Unione è competente a determinare i compiti di Eurojust ed Europol, rispettivamente.

- **Sussidiarietà**

Ai fini della libertà di circolazione all'interno dell'UE è necessaria una gestione efficace delle frontiere esterne dell'Unione mirante a garantire la sicurezza. Gli Stati membri hanno pertanto convenuto di affrontare insieme queste sfide, in particolare scambiandosi informazioni tramite sistemi centralizzati dell'UE nel settore della giustizia e degli affari interni. Lo confermano le varie conclusioni adottate sia dal Consiglio europeo che dal Consiglio, soprattutto a partire dal 2015.

L'assenza di controlli alle frontiere interne richiede una corretta gestione delle frontiere esterne dello spazio Schengen in cui ogni Stato membro, o paese associato Schengen, sia tenuto a controllare la propria frontiera esterna per conto degli altri Stati Schengen. Di conseguenza, nessuno Stato membro è in grado di far fronte, da solo, alla migrazione irregolare e alla criminalità transfrontaliera. I cittadini di paesi terzi che entrano in questo spazio privo di controlli alle frontiere interne possono spostarsi liberamente al suo interno. In uno spazio senza frontiere interne, qualunque azione contro l'immigrazione irregolare e la criminalità e il terrorismo internazionali, anche attraverso l'individuazione delle frodi di identità, andrebbe intrapresa congiuntamente e può avere successo solo se portata avanti a livello dell'UE.

A tale livello esistono già o stanno per essere introdotti sistemi di informazione comuni di cruciale importanza. Una maggior interoperabilità fra tali sistemi comporta necessariamente un'azione a livello dell'UE. La proposta ha come obiettivo centrale quello di migliorare l'efficienza e l'uso dei sistemi centralizzati gestiti da eu-LISA. Le azioni previste hanno una portata, degli effetti e un impatto tali da rendere possibile il raggiungimento efficace e sistematico degli obiettivi fondamentali solo a livello dell'UE.

- **Proporzionalità**

Come illustrato con dovizia di dettagli nella valutazione d'impatto che accompagna la presente proposta di regolamento, le scelte strategiche operate nella presente proposta sono ritenute proporzionate e non vanno al di là di quanto necessario per il raggiungimento degli obiettivi concordati.

Il **portale di ricerca europeo (ESP)** è uno strumento necessario per rafforzare l'uso autorizzato dei sistemi di informazione dell'UE attuali e futuri. Il suo impatto in termini di trattamento dei dati è molto limitato. L'ESP non conserverà alcun dato, tranne le informazioni riguardanti i diversi profili dei suoi utenti, nonché i dati e i sistemi di informazione cui essi hanno accesso, tenendo traccia del loro utilizzo mediante registrazioni. Il ruolo dell'ESP come mediatore di messaggi, catalizzatore e facilitatore è proporzionato, necessario e limitato per quel che riguarda le ricerche e i diritti di accesso, in virtù dei mandati delle basi giuridiche relative ai sistemi di informazione e della proposta di regolamento sull'interoperabilità.

Il **servizio comune di confronto biometrico (BMS comune)** è necessario per il funzionamento dell'ESP, dell'archivio comune di dati di identità e del rilevatore di identità multiple e facilita l'uso e la manutenzione dei sistemi di informazione dell'UE pertinenti, attuali e futuri. Le sue funzioni consentono di effettuare ricerche su dati biometrici provenienti da fonti diverse in modo efficace, continuato e sistematico. I dati biometrici sono archiviati e conservati dai sistemi sottostanti. Il BMS comune crea dei template, ma rimuove le immagini reali. I dati sono pertanto conservati in un unico luogo, una volta sola.

L'**archivio comune di dati di identità (CIR)** è necessario per identificare correttamente un cittadino di paese terzo, ad esempio durante una verifica di identità nello spazio Schengen. Il CIR serve inoltre da supporto al funzionamento del rilevatore di identità multiple ed è pertanto una componente necessaria per conseguire il duplice obiettivo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. L'accesso al CIR per tali finalità è limitato agli utenti che hanno bisogno delle informazioni così accessibili per svolgere le loro mansioni (di qui la necessità di includere tali verifiche quale nuova finalità accessoria dell'Eurodac, del VIS, del futuro EES e dell'ETIAS e del sistema ECRIS-TCN proposti). Il trattamento dei dati è rigorosamente limitato a quanto necessario per conseguire detto obiettivo e saranno introdotte garanzie adeguate per far sì che i diritti di accesso siano rispettati e che i dati conservati nel CIR siano ridotti allo stretto indispensabile. Per garantire la minimizzazione dei dati ed evitare duplicazioni ingiustificate, il CIR detiene, senza copiarli, i dati anagrafici necessari di ciascuno dei sistemi sottostanti - che vengono conservati, aggiunti, modificati e cancellati in conformità della rispettiva base giuridica. Le condizioni di conservazione dei dati risultano pienamente in linea con le disposizioni previste in tal senso dal sistema di informazione sottostante da cui provengono i dati di identità.

Il **rilevatore di identità multiple (MID)** è necessario quale soluzione per l'individuazione delle identità multiple, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. Conterrà i collegamenti tra le persone fisiche presenti in più di un sistema di informazione centrale, limitandosi rigorosamente ai dati necessari per accertare se l'interessato è lecitamente o illecitamente registrato con identità anagrafiche diverse in sistemi diversi, ma servirà anche a chiarire i casi in cui due persone aventi dati anagrafici simili possono non essere la stessa persona. Il trattamento dei dati tramite il MID e il BMS comune al fine di collegare i fascicoli individuali trasversalmente ai singoli sistemi si limiterà al minimo indispensabile. Il MID includerà misure di salvaguardia contro eventuali discriminazioni o decisioni sfavorevoli nei confronti di persone con identità multiple lecite.

- **Scelta dell'atto giuridico**

L'atto giuridico proposto è un regolamento del Parlamento europeo e del Consiglio. La legislazione proposta riguarda direttamente il funzionamento dei sistemi di informazione centrali dell'UE per la gestione delle frontiere e la sicurezza, tutti già istituiti tramite regolamenti o la cui istituzione è proposta in tale forma. Tramite un regolamento è stata istituita anche eu-LISA, che sarà responsabile della progettazione e dello sviluppo delle componenti e, a tempo debito, della loro gestione tecnica. Un regolamento è pertanto l'atto giuridico idoneo.

3. RISULTATI DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- **Consultazione pubblica**

Nel luglio 2017, in vista della preparazione della presente proposta, la Commissione ha avviato una consultazione pubblica per raccogliere i pareri dei portatori di interessi in materia di interoperabilità. Sono pervenute 18 risposte da parte di un'ampia gamma di portatori di interessi, tra cui governi degli Stati membri, organizzazioni del settore privato, altre organizzazioni quali le ONG e i gruppi di riflessione, nonché privati cittadini[33]. In generale, i partecipanti alla consultazione si sono espressi sostanzialmente a favore dei principi alla base della presente proposta di interoperabilità e, nella stragrande maggioranza, hanno convenuto sulla correttezza delle questioni sollevate dalla consultazione e degli obiettivi perseguiti dal pacchetto sull'interoperabilità. A loro avviso, in particolare, le opzioni descritte nel documento di consultazione avrebbero permesso di:

- aiutare il personale sul campo ad accedere alle informazioni di cui ha bisogno;
- evitare la duplicazione dei dati, ridurre le sovrapposizioni ed evidenziare eventuali discrepanze fra i dati;
- identificare le persone, anche quelle con identità multiple, con un maggior grado di attendibilità e ridurre la frode di identità.

Nelle risposte fornite, una netta maggioranza si è detta a favore di ciascuna delle opzioni proposte, ritenute necessarie per conseguire gli obiettivi della presente iniziativa, e ha sottolineato l'esigenza di misure rigorose e chiare in materia di protezione dei dati, in particolare per quanto concerne l'accesso alle informazioni archiviate nei sistemi e la conservazione dei dati, nonché la necessità di dati aggiornati e di alta qualità nei sistemi e, a tal fine, di apposite misure.

Tutti i punti sollevati sono stati presi in considerazione all'atto della preparazione della presente proposta.

- **Indagine Eurobarometro**

Nel giugno 2017 è stato realizzato un sondaggio speciale Eurobarometro[34] che ha evidenziato l'ampio sostegno dei cittadini alla strategia dell'UE in materia di scambio delle informazioni a livello di Unione a fini di contrasto della criminalità e del terrorismo: quasi tutti gli intervistati (il 92 %) hanno convenuto sull'opportunità che le autorità nazionali scambino le informazioni con le autorità degli altri Stati membri, al fine di rendere più efficace tale azione di contrasto.

Secondo una netta maggioranza degli intervistati (il 69 %), la polizia e le altre autorità di contrasto nazionali dovrebbero scambiare le informazioni con gli altri paesi dell'UE in modo sistematico. In tutti gli Stati membri, la maggioranza degli intervistati ritiene che le informazioni dovrebbero essere scambiate in ogni singolo caso.

---

[33] Ulteriori dettagli sono contenuti nella relazione di sintesi allegata alla valutazione d'impatto.

[34] La relazione *Europeans' attitudes towards security* analizza i risultati del sondaggio speciale di opinione Eurobarometro (464b) per quanto riguarda il grado di consapevolezza generale, le esperienze e le percezioni dei cittadini relativamente alla sicurezza. Il sondaggio è stato condotto dalla rete TNS "Political & Social" nei 28 Stati membri, tra il 13 e il 26 giugno 2017. Sono stati intervistati circa 28 093 cittadini UE di estrazioni sociali e categorie demografiche diverse.

- **Gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità**

Come già precisato nell'introduzione, la presente proposta si basa sulle raccomandazioni del **gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità**[35]. Il gruppo, istituito nel giugno 2016 con l'obiettivo di affrontare i problemi di ordine giuridico, tecnico e operativo delle opzioni disponibili per realizzare l'interoperabilità tra i sistemi centrali dell'UE riguardanti le frontiere e la sicurezza, ha adottato una prospettiva ampia e globale in materia di architettura di gestione dei dati per la gestione delle frontiere e il contrasto, tenendo conto anche dei ruoli, delle responsabilità e dei sistemi pertinenti per le autorità doganali.

Il gruppo ha riunito esperti degli Stati membri, dei paesi associati Schengen e delle seguenti agenzie dell'UE: eu-LISA, Europol, Ufficio europeo di sostegno per l'asilo, Agenzia europea della guardia di frontiera e costiera e Agenzia dell'UE per i diritti fondamentali. Hanno partecipato, in qualità di membri a pieno titolo, anche il coordinatore antiterrorismo dell'UE e il garante europeo della protezione dei dati e, in qualità di osservatori, rappresentanti del segretariato della commissione del Parlamento europeo per le libertà civili, la giustizia e gli affari interni e del segretariato generale del Consiglio.

Nella **relazione finale** pubblicata nel maggio 2017[36] **il gruppo di esperti ad alto livello** ha sottolineato la necessità di agire per sopperire alle lacune strutturali identificate nella comunicazione dell'aprile 2016 e ha formulato una serie di raccomandazioni volte a rafforzare e sviluppare i sistemi di informazione dell'UE e la loro interoperabilità. Ha concluso che era **necessario e tecnicamente fattibile adoperarsi per introdurre il portale di ricerca europeo, il servizio comune di confronto biometrico e l'archivio comune di dati di identità quali soluzioni di interoperabilità** e che, in linea di massima, tali componenti erano in grado di offrire vantaggi operativi e di essere istituite nel rispetto dei requisiti in materia di protezione dei dati. Ha infine raccomandato di esaminare anche l'opzione supplementare di un approccio in due fasi per l'accesso a fini di contrasto, basato su una funzione di segnalazione "hit/no hit".

La presente proposta di regolamento risponde inoltre alle raccomandazioni formulate dal gruppo di esperti sulla qualità dei dati, sul formato universale dei messaggi (UMF) e sulla creazione di un archivio di dati (qui presentato come archivio centrale di relazioni e statistiche, o CRRS).

La quarta componente dell'interoperabilità proposta (il rilevatore di identità multiple) non era stata menzionata dal gruppo di esperti; la questione è emersa nel corso di ulteriori analisi tecniche e nel quadro della valutazione della proporzionalità effettuata dalla Commissione.

- **Studi tecnici**

A sostegno della preparazione della proposta sono stati commissionati tre studi. Sulla base di un contratto stipulato con la Commissione, Unisys ha presentato una relazione riguardante uno studio di fattibilità per il portale di ricerca europeo. eu-LISA ha commissionato a Gartner (in collaborazione con Unisys) una relazione tecnica per contribuire allo sviluppo del servizio comune di confronto biometrico. PWC ha infine presentato alla Commissione una relazione tecnica su un archivio comune di dati di identità.

---

[35] Decisione della Commissione del 17 giugno 2016 che istituisce il gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità — 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

- **Valutazione d'impatto**

La presente proposta è corredata di una valutazione d'impatto, presentata nel documento di lavoro dei servizi della Commissione SWD(2017) XXX che la accompagna.

Nella riunione del 6 dicembre 2017 il comitato per il controllo normativo ha esaminato il progetto di valutazione d'impatto e, l'8 dicembre, ha formulato un parere (favorevole, con riserve) indicando la necessità di modificare tale valutazione per tener conto delle sue raccomandazioni su alcuni aspetti specifici. Le raccomandazioni riguardavano, innanzitutto, misure supplementari nell'ambito dell'opzione prescelta intese a semplificare gli attuali diritti di accesso degli utenti finali ai dati contenuti nei sistemi di informazione dell'UE e a specificare le relative garanzie connesse alla protezione dei dati e ai diritti fondamentali. La seconda considerazione fondamentale consisteva in una richiesta di chiarimento delle modalità di integrazione del sistema di informazione Schengen nell'opzione 2, inclusa l'efficacia e i costi, per facilitarne il raffronto con l'opzione 3 prescelta. La Commissione ha aggiornato la valutazione d'impatto per tener conto di queste considerazioni principali e per rispondere a una serie di altre osservazioni formulate dal comitato.

La valutazione d'impatto ha analizzato se e in quale misura ciascuno degli obiettivi previsti poteva essere conseguito utilizzando una o più delle componenti tecniche individuate dal gruppo di esperti ad alto livello e tramite un'analisi successiva. All'occorrenza, ha anche preso in esame le sotto-opzioni necessarie per conseguire tali obiettivi, nel rispetto delle norme sulla protezione dei dati. La valutazione ha concluso che:

- per conseguire l'obiettivo di fornire agli utenti autorizzati un accesso rapido, continuato, sistematico e controllato ai sistemi di informazione pertinenti, era opportuno creare un portale di ricerca europeo (ESP) basato su un servizio comune di confronto biometrico (BMS comune) che permettesse l'interrogazione di tutte le banche dati;
- per conseguire l'obiettivo di agevolare, nel territorio di uno Stato membro, le verifiche di identità dei cittadini di paesi terzi da parte degli operatori autorizzati, era opportuno creare un archivio comune di dati di identità (CIR) contenente un insieme minimo di dati identificativi, anch'esso basato sul BMS comune;
- per conseguire l'obiettivo di rilevare le identità multiple collegate alla stessa serie di dati biometrici, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità, era opportuno creare un rilevatore di identità multiple (MID) contenente collegamenti tra le identità multiple presenti nei diversi sistemi;
- per conseguire l'obiettivo di agevolare e semplificare l'accesso delle autorità di contrasto a sistemi di informazione estranei al settore del contrasto a fini di prevenzione, indagine, accertamento o perseguimento di reati gravi e di terrorismo, era opportuno includere nel CIR una funzione di segnalazione basata su riscontri positivi e negativi ("hit/no hit").

Poiché occorre conseguire tutti i suddetti obiettivi, **la soluzione ottimale consiste in una combinazione delle componenti ESP, CIR (provvisto di una funzione di segnalazione "hit/no hit") e MID, tutte basate sul BMS comune**.

L'impatto positivo principale sarà il miglioramento della gestione delle frontiere e una maggior sicurezza all'interno dell'Unione europea. Le nuove componenti renderanno più

semplice e veloce l'accesso delle autorità nazionali alle informazioni necessarie e l'identificazione dei cittadini di paesi terzi. Permetteranno alle autorità di effettuare collegamenti incrociati tra le informazioni necessarie preesistenti sulle persone fisiche al momento delle verifiche di frontiera, della presentazione delle domande di asilo e di visto e per le attività di polizia. In tal modo consentiranno di accedere a informazioni che permetteranno di adottare decisioni attendibili in relazione ad indagini su reati gravi e di terrorismo o in materia di migrazione e di asilo. Pur non riguardando direttamente i cittadini dell'UE, ma essenzialmente i cittadini di paesi terzi i cui dati sono registrati in un sistema di informazione centralizzato dell'UE, le misure proposte dovrebbero accrescere la fiducia dell'opinione pubblica garantendo, mediante la loro concezione e il loro utilizzo, maggior sicurezza ai cittadini dell'UE.

L'impatto economico e finanziario immediato della proposta sarà limitato alla progettazione, allo sviluppo e al funzionamento dei nuovi strumenti. I costi ricadranno sul bilancio dell'UE e sulle autorità degli Stati membri responsabili del funzionamento dei vari sistemi. L'impatto sul turismo sarà positivo, poiché le misure proposte non solo miglioreranno la sicurezza dell'Unione europea, ma dovrebbero anche rendere più veloci i controlli di frontiera. Rendendo più veloci i controlli di frontiera, la proposta dovrebbe avere un impatto positivo anche sugli aeroporti, sui porti marittimi e sui vettori.

- **Diritti fondamentali**

La valutazione d'impatto ha esaminato l'incidenza delle misure proposte sui diritti fondamentali e, in particolare, sul diritto alla protezione dei dati.

Conformemente alla Carta dei diritti fondamentali dell'Unione europea, che vincola sia le istituzioni dell'UE che gli Stati membri nell'attuazione del diritto dell'Unione (articolo 51, paragrafo 1, della Carta), le opportunità offerte dall'interoperabilità quale misura volta a migliorare la sicurezza e la protezione delle frontiere esterne devono conciliarsi con l'obbligo di garantire che le ingerenze nei diritti fondamentali eventualmente generate dal nuovo contesto di interoperabilità si limitino a quanto strettamente necessario per rispondere effettivamente alle finalità di interesse generale perseguite, nel rispetto del principio di proporzionalità (articolo 52, paragrafo 1, della Carta).

Le soluzioni di interoperabilità proposte sono componenti complementari ai sistemi esistenti. In quanto tali, esse non andranno ad intaccare l'equilibrio già garantito da ciascuno dei sistemi centrali esistenti per quanto riguarda il loro impatto positivo sui diritti fondamentali.

L'interoperabilità, tuttavia, ha di fatto la capacità di incidere ulteriormente, in maniera indiretta, su una serie di diritti fondamentali. Se, da un lato, la corretta identificazione di una persona ha un impatto positivo sul diritto al rispetto della vita privata e, in particolare, sul diritto alla propria identità (articolo 7 della Carta), poiché può contribuire a evitare confusioni sull'identità, dall'altro le verifiche basate sui dati biometrici possono essere percepite come un'ingerenza nel diritto alla dignità umana (in particolare, se ritenute umilianti) (articolo 1). Tuttavia, in un'indagine condotta dall'Agenzia dell'UE per i diritti fondamentali[37] è stato chiesto specificamente agli intervistati se ritenessero umiliante fornire i loro dati biometrici nell'ambito di un controllo di frontiera. La maggioranza ha risposto di no.

[37] *FRA survey in the framework of the eu-LISA pilot on smart borders — travellers' views on and experiences of smart borders*, relazione dell'Agenzia dell'Unione europea per i diritti fondamentali (testo disponibile solo in inglese): http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

Le componenti dell'interoperabilità proposte offrono la possibilità di adottare misure preventive mirate, allo scopo di aumentare la sicurezza. In quanto tali, possono contribuire alla protezione del diritto delle persone alla vita (articolo 2 della Carta), il che implica contemporaneamente l'obbligo positivo per le autorità di adottare misure operative di prevenzione volte a proteggere la persona la cui vita sia a rischio, qualora esse siano a conoscenza, o avrebbero dovuto essere a conoscenza, dell'esistenza di un rischio immediato[38], e di far rispettare la proibizione della schiavitù e del lavoro forzato (articolo 5). Grazie a un'identificazione attendibile, più accessibile e più semplice, l'interoperabilità può favorire l'individuazione dei minori scomparsi o vittime della tratta di esseri umani e favorire reazioni rapide e mirate.

Un'identificazione attendibile, più accessibile e più semplice potrebbe inoltre contribuire a garantire il rispetto effettivo del diritto di asilo (articolo 18 della Carta) e del divieto di allontanamento (articolo 19 della Carta). L'interoperabilità, infatti, potrebbe evitare che un richiedente asilo venga fermato e trattenuto illegalmente e assoggettato ad un provvedimento di espulsione ingiustificato. Grazie all'interoperabilità sarà inoltre più facile scoprire la frode di identità. Si ridurrà infine la necessità di scambiare con i paesi terzi (in particolare, con il paese d'origine) dati e informazioni sul richiedente asilo al fine di stabilirne l'identità e di ottenere i documenti di viaggio, il che potrebbe mettere potenzialmente in pericolo l'interessato.

- **Protezione dei dati personali**

Poiché riguarderà i dati personali, l'interoperabilità inciderà soprattutto sul diritto alla loro protezione. Tale diritto è affermato dall'articolo 8 della Carta e dall'articolo 16 del trattato sul funzionamento dell'Unione europea, nonché dall'articolo 8 della Convenzione europea dei diritti dell'uomo. Come sottolineato dalla Corte di giustizia dell'Unione europea[39], il diritto alla protezione dei dati personali non appare come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale[40]. La protezione dei dati è strettamente legata al rispetto della vita privata e familiare tutelato dall'articolo 7 della Carta.

Secondo il regolamento generale sulla protezione dei dati[41], la libera circolazione dei dati all'interno dell'UE non deve essere limitata per motivi legati alla protezione dei dati. Occorre tuttavia rispettare una serie di principi. Di fatto, per essere lecite, le eventuali limitazioni all'esercizio dei diritti fondamentali tutelati dalla Carta devono rispondere ai seguenti criteri, sanciti dall'articolo 52, paragrafo 1:

- devono essere previste dalla legge,
- devono rispettare il contenuto essenziale dei diritti,

[38] Corte europea dei diritti dell'uomo, Salih Osman contro Regno Unito, sentenza n. 87/1997/871/1083, del 28 ottobre 1998, punto 116.

[39] Sentenza della Corte di giustizia dell'Unione europea del 9 novembre 2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert, [2010] ECR I-0000.

[40] Conformemente all'articolo 52, paragrafo 1, della Carta, possono essere apportate limitazioni all'esercizio del diritto alla protezione dei dati purché esse siano previste dalla legge, rispettino il contenuto essenziale dei diritti e delle libertà e, in ottemperanza al principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

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

- devono rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui,
- devono essere necessarie,
- devono essere proporzionate.

La presente proposta di regolamento tiene conto di tutte queste norme in materia di protezione dei dati, come indicato con dovizia di dettagli nella valutazione d'impatto che la accompagna, ed è basata sui principi della protezione dei dati fin dalla progettazione e per impostazione predefinita. Comprende tutte le opportune disposizioni che limitano il trattamento dei dati a quanto necessario per lo scopo specifico da conseguire e che concedono l'accesso ai dati soltanto ai soggetti che hanno la "necessità di sapere". I periodi di conservazione dei dati (se del caso) sono adeguati e di durata limitata. L'accesso ai dati è riservato esclusivamente al personale debitamente autorizzato delle autorità degli Stati membri o degli organi dell'UE competenti per gli scopi specifici di ciascun sistema di informazione ed è limitato alla necessità di tali dati per l'esecuzione dei compiti connessi al conseguimento degli scopi predetti.

4. INCIDENZA SUL BILANCIO

L'incidenza sul bilancio è riportata nella scheda finanziaria allegata, riguardante il periodo rimanente dell'attuale quadro finanziario pluriennale (fino al 2020), nonché i sette anni del periodo successivo (2021-2027). La dotazione proposta per gli anni dal 2021 in poi è inclusa a fini illustrativi e non pregiudica il prossimo quadro finanziario pluriennale.

L'attuazione della presente proposta richiederà stanziamenti di bilancio per:

(1) lo **sviluppo** e l'integrazione, da parte di eu-LISA, delle quattro componenti dell'interoperabilità e dell'archivio centrale di relazioni e statistiche e, successivamente, **la loro manutenzione e il loro funzionamento**;

(2) la **migrazione dei dati** verso il servizio comune di confronto biometrico (BMS comune) e l'archivio comune di dati di identità (CIR). All'interno del BMS comune occorre ricreare i template biometrici dei dati corrispondenti ricavati dai tre sistemi che attualmente utilizzano rilevazioni biometriche (SIS, VIS ed Eurodac). Per quanto riguarda il CIR occorre realizzare la migrazione verso di esso degli elementi dei dati personali ricavati dal VIS e convalidare i collegamenti eventualmente individuati tra le identità presenti nel SIS, nel VIS e nell'Eurodac. Quest'ultimo processo, in particolare, comporta un ingente dispendio di risorse;

(3) l'aggiornamento, da parte di eu-LISA, dell'**interfaccia uniforme nazionale** (NUI) già inclusa nel regolamento EES, così che essa diventi una componente generica in grado di consentire lo scambio di messaggi tra gli Stati membri e il sistema/i sistemi centrali;

(4) l'**integrazione dei sistemi nazionali degli Stati membri** con la NUI, che trasmetterà i messaggi scambiati con il CIR e con il rilevatore di identità multiple attraverso il portale di ricerca europeo;

(5) la **formazione** degli utenti finali all'uso delle componenti dell'interoperabilità, anche tramite l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL).

La creazione e la manutenzione delle componenti dell'interoperabilità sono effettuate in quanto programma. Mentre il portale di ricerca europeo (ESP) e il rilevatore di identità multiple, unitamente all'archivio centrale di relazioni e statistiche (CRRS), sono componenti totalmente nuove, il BMS comune e il CIR sono componenti condivise che combinano dati precedentemente archiviati (o da archiviare) in sistemi già funzionanti o nuovi, per i quali esistono già stime di bilancio specifiche.

L'**ESP** implementerà le interfacce con il SIS, il VIS e l'Eurodac già note e preesistenti e, a tempo debito, sarà esteso a nuovi sistemi.

L'ESP sarà utilizzato dagli Stati membri e dalle agenzie mediante un'interfaccia basata sul formato universale dei messaggi (UMF). Questa nuova interfaccia dovrà essere sviluppata, adattata, integrata e testata dagli Stati membri, da eu-LISA, da Europol e dall'Agenzia europea della guardia di frontiera e costiera. L'ESP dovrebbe utilizzare i concetti di interfaccia uniforme nazionale (NUI) introdotti per l'EES, riducendo in tal modo gli sforzi di integrazione.

Per Europol l'ESP genererà costi supplementari, necessari per rendere l'interfaccia QUEST utilizzabile con dati aventi un livello di protezione minimo (LPM).

La base del **BMS comune** sarà di fatto istituita con la creazione del nuovo EES, poiché quest'ultimo conterrà il volume di gran lunga maggiore di nuovi dati biometrici. La dotazione necessaria è stata stanziata nell'ambito dello strumento giuridico dell'EES. L'aggiunta al BMS comune di ulteriori dati biometrici ricavati dal VIS, dal SIS e dall'Eurodac rappresenta un costo supplementare principalmente connesso alla migrazione dei dati esistenti. Il costo stimato è di 10 milioni di EUR per tutti e tre i sistemi. L'aggiunta di nuovi dati biometrici ricavati dal sistema ECRIS-TCN proposto rappresenta invece un costo supplementare limitato che può essere coperto dai finanziamenti previsti dallo strumento giuridico ECRIS-TCN per l'istituzione del sistema automatico di identificazione dattiloscopica ECRIS-TCN.

L'**archivio comune di dati di identità** sarà istituito con la creazione del futuro EES e ulteriormente ampliato all'atto dello sviluppo dell'ETIAS proposto. I motori di archiviazione e di ricerca per questi dati sono stati inclusi nella dotazione prevista nell'ambito degli strumenti giuridici del futuro EES e dell'ETIAS proposto. L'aggiunta di nuovi dati anagrafici ricavati sia dall'Eurodac che dal sistema ECRIS-TCN proposto comporta un costo supplementare minimo già previsto nell'ambito degli strumenti giuridici dell'Eurodac e del sistema ECRIS-TCN proposto.

La dotazione totale necessaria per un periodo di nove anni (2019-2027) ammonta a 424,7 milioni di EUR, così ripartiti:

(1) una dotazione pari a 225 milioni di EUR a favore di eu-LISA, che copre il costo totale per lo sviluppo del programma che realizza le cinque componenti dell'interoperabilità (68,3 milioni di EUR), i costi di manutenzione di dette componenti fino al 2027 a partire dal momento della loro realizzazione (56,1 milioni di EUR), una dotazione specifica di 25 milioni di EUR per la migrazione dei dati dai sistemi esistenti al BMS comune e i costi aggiuntivi per l'aggiornamento, la rete, la formazione e le riunioni connessi alla NUI. Una dotazione specifica di 18,7 milioni di EUR copre i costi di adeguamento e di funzionamento dell'ECRIS-TCN in modalità ad alta disponibilità a partire dal 2022;

(2) una dotazione pari a 136,3 milioni di EUR per permettere agli Stati membri di

coprire i costi delle modifiche ai rispettivi sistemi nazionali necessarie per utilizzare le componenti dell'interoperabilità e l'interfaccia NUI fornita da eu-LISA e per la formazione di una folta comunità di utenti;

(3) una dotazione pari a 48,9 milioni di EUR per Europol, destinata a coprire i costi di adeguamento dei sistemi informatici di Europol al volume di messaggi da trattare e all'aumento dei livelli di prestazione[42]. Le componenti dell'interoperabilità saranno utilizzate dall'ETIAS per consultare i dati Europol;

(4) una dotazione pari a 4,8 milioni di EUR a favore dell'Agenzia europea della guardia di frontiera e costiera per ospitare un gruppo di esperti incaricati di convalidare, nell'arco di un anno, i collegamenti tra identità, quando il rilevatore di identità multiple sarà entrato in funzione;

(5) una dotazione pari a 2,0 milioni di EUR a favore dell'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL) destinata a coprire i costi della preparazione e della realizzazione di corsi di formazione per il personale operativo;

(6) uno stanziamento di 7,7 milioni di EUR per la DG HOME destinato a coprire un aumento limitato di personale e i relativi costi durante il periodo di sviluppo delle diverse componenti, dal momento che la Commissione dovrà anch'essa svolgere compiti supplementari nel corso di tale periodo e sarà responsabile del comitato che si occuperà del formato universale dei messaggi.

Il regolamento riguardante il Fondo sicurezza interna (ISF)-Frontiere è lo strumento finanziario in cui è stata inclusa la dotazione destinata all'attuazione dell'iniziativa sull'interoperabilità. All'articolo 5, lettera b), esso prevede che 791 milioni di EUR siano utilizzati nell'ambito di un programma per lo sviluppo di sistemi informatici basati su sistemi attuali e/o nuovi a sostegno della gestione dei flussi migratori attraverso le frontiere esterne, previa adozione dei pertinenti atti legislativi dell'Unione e conformemente alle condizioni di cui all'articolo 15, paragrafo 5. Di questo importo, 480,2 milioni di EUR sono destinati allo sviluppo dell'EES, 210 milioni di EUR all'ETIAS e 67,9 milioni di EUR alla revisione del SIS. La cifra restante (32,9 milioni di EUR) dovrà essere riassegnata utilizzando i meccanismi dell'ISF-Frontiere. Per il rimanente periodo (2019-2020) coperto dal quadro finanziario pluriennale attuale, la presente proposta necessita di una dotazione pari a 32,1 milioni di EUR, vale a dire un importo rientrante nella dotazione restante.

5. INFORMAZIONI SUPPLEMENTARI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

eu-LISA è responsabile della gestione operativa dei sistemi informatici su larga scala nello spazio di libertà, sicurezza e giustizia. In quanto tale, è sin d'ora incaricata dell'esercizio e dei miglioramenti tecnici e operativi dei sistemi esistenti, nonché dello sviluppo dei sistemi futuri già previsti. Ai sensi della presente proposta di regolamento, essa definirà la progettazione dell'architettura fisica delle componenti dell'interoperabilità, le svilupperà ed attuerà e, infine, le ospiterà. Le rispettive componenti saranno attuate progressivamente, parallelamente allo sviluppo dei sistemi sottostanti.

[42] Attualmente Europol ha una capacità di trattamento delle informazioni non adatta ai grandi volumi (in media, 100 000 interrogazioni al giorno) e ai tempi di risposta più brevi richiesti dall'ETIAS.

La Commissione farà sì che siano istituiti sistemi atti a monitorare lo sviluppo e il funzionamento delle quattro componenti (portale di ricerca europeo, servizio comune di confronto biometrico, archivio comune di dati di identità e rilevatore di identità multiple) e dell'archivio centrale di relazioni e statistiche e provvederà ad una loro valutazione in base ai principali obiettivi strategici. Quattro anni dopo l'introduzione e l'avvio operativo delle varie funzionalità e, in seguito, ogni quattro anni, eu-LISA dovrà presentare al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico delle componenti dell'interoperabilità. Inoltre, cinque anni dopo l'introduzione e l'avvio operativo delle varie funzionalità e, in seguito, ogni quattro anni, la Commissione dovrebbe predisporre una valutazione generale delle componenti, riguardante anche il loro impatto diretto o indiretto e l'incidenza della loro attuazione pratica sui diritti fondamentali. Essa dovrebbe esaminare i risultati conseguiti rispetto agli obiettivi, valutando nel contempo se i principi di base sono ancora validi e studiando le eventuali implicazioni per le opzioni future. La Commissione dovrebbe presentare le relazioni di valutazione al Parlamento europeo e al Consiglio.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

Il capo I prevede le disposizioni generali del presente regolamento. Ne illustra i principi di fondo, le componenti che vi sono istituite, gli obiettivi che l'interoperabilità si prefigge di realizzare e l'ambito di applicazione; definisce i termini utilizzati e stabilisce il principio di non discriminazione in materia di trattamento dei dati ai sensi del regolamento stesso.

Il capo II contiene le disposizioni relative al portale di ricerca europeo (ESP). Ne prevede l'istituzione e ne definisce l'architettura tecnica, che dovrà essere sviluppata da eu-LISA. Precisa la finalità dell'ESP e individua chi può farne uso e con quali modalità, nel rispetto dei diritti di accesso esistenti per ciascuno dei sistemi centrali. Prevede inoltre che eu-LISA crei dei profili per ogni categoria di utenti. Il capo II illustra in che modo l'ESP interrogherà i sistemi centrali e contiene disposizioni riguardanti il contenuto e il formato delle risposte agli utenti. Dispone anche che eu-LISA conservi le registrazioni di tutte le operazioni di trattamento e definisce la procedura sostitutiva da applicare qualora l'ESP non sia in grado di accedere a uno o più sistemi centrali.

Il capo III contiene le disposizioni relative al servizio comune di confronto biometrico (BMS comune). Ne prevede l'istituzione e ne definisce l'architettura tecnica, che dovrà essere sviluppata da eu-LISA. Precisa la finalità del BMS comune e stabilisce quali dati vi saranno conservati. Spiega la relazione tra il BMS comune e le altre componenti. Stabilisce infine che il BMS comune non continuerà a conservare i dati dopo la loro rimozione dal rispettivo sistema centrale e dispone che eu-LISA conservi le registrazioni di tutte le operazioni di trattamento.

Il capo IV contiene le disposizioni relative all'archivio comune di dati di identità (CIR). Ne prevede l'istituzione e ne definisce l'architettura tecnica, che dovrà essere sviluppata da eu-LISA. Ne precisa la finalità e chiarisce quali dati vi saranno conservati e con quali modalità, comprese le disposizioni volte a garantire la qualità dei dati conservati. Prevede che il CIR crei fascicoli individuali sulla base dei dati contenuti nei sistemi centrali e che tali fascicoli siano aggiornati in funzione delle modifiche apportate nei singoli sistemi centrali. Specifica inoltre le modalità di funzionamento dell'archivio in relazione al rilevatore di identità multiple. Individua chi può accedervi e con quali modalità sarà possibile accedere ai dati, nel rispetto dei relativi diritti, e prevede disposizioni più specifiche a seconda che la finalità consista nell'identificazione o, quale primo stadio dell'approccio in due fasi, nell'accesso all'EES, al VIS, all'ETIAS e all'Eurodac tramite il CIR a fini di contrasto. Dispone infine che eu-LISA conservi le registrazioni di tutte le operazioni di trattamento concernenti il CIR.

Il capo V contiene le disposizioni relative al rilevatore di identità multiple (MID). Ne prevede l'istituzione e ne definisce l'architettura tecnica, che dovrà essere sviluppata da eu-LISA. Ne spiega la finalità e ne disciplina l'utilizzo in conformità dei diritti d'accesso a ciascuno dei sistemi centrali. Definisce quando e in che modo il MID avvierà una ricerca per individuare la presenza di identità multiple, con quali modalità verranno forniti i risultati e come vi sarà dato seguito, se necessario anche mediante verifica manuale. Classifica i tipi di collegamento eventualmente generati da una ricerca a seconda che il risultato indichi un'identità singola, identità multiple o identità condivise. Stabilisce che il MID conservi i dati oggetto del collegamento archiviati nei sistemi centrali fintantoché tali dati permarranno in due o più singoli sistemi centrali. Dispone infine che eu-LISA conservi le registrazioni di tutte le operazioni di trattamento dei dati concernenti il MID.

Il capo VI prevede misure a sostegno dell'interoperabilità. Prevede il miglioramento della qualità dei dati, stabilisce il formato universale dei messaggi quale standard comune per lo scambio di informazioni a sostegno dell'interoperabilità e istituisce un archivio centrale di relazioni e statistiche.

Il capo VII riguarda la protezione dei dati. Introduce disposizioni volte a garantire che il trattamento dei dati nel quadro del presente regolamento avvenga in modo lecito e appropriato, in linea con le disposizioni del regolamento (CE) n. 45/2001. Spiega chi sarà responsabile del trattamento dei dati per ciascuna misura di interoperabilità proposta nel presente regolamento e stabilisce le misure richieste ad eu-LISA e alle autorità degli Stati membri per garantire la sicurezza del trattamento dei dati, la loro riservatezza, la gestione appropriata degli incidenti di sicurezza e il monitoraggio adeguato del rispetto delle misure previste dal presente regolamento. Contiene inoltre disposizioni relative ai diritti di coloro cui si riferiscono i dati, tra cui il diritto a essere informati della conservazione e del trattamento di dati che li riguardano a norma del presente regolamento e il diritto di accedere, rettificare e cancellare i dati personali conservati e trattati nell'ambito del presente regolamento. Il capo VII stabilisce inoltre il principio in base al quale i dati trattati ai sensi del presente regolamento non devono essere trasferiti né messi a disposizione di un paese terzo, di un'organizzazione internazionale o di un soggetto privato, ad eccezione dell'Interpol, per alcuni scopi specifici, e dei dati ricevuti da Europol attraverso il portale di ricerca europeo, ai quali si applicano le norme del regolamento 2016/794 sul successivo trattamento dei dati. Contiene infine disposizioni riguardanti la vigilanza e l'audit in relazione alla protezione dei dati.

Il capo VIII stabilisce le responsabilità di eu-LISA prima e dopo l'entrata in funzione delle misure di cui alla presente proposta, nonché degli Stati membri, di Europol e dell'unità centrale ETIAS.

Il capo IX fornisce dettagli riguardanti: le norme di elaborazione di statistiche e relazioni concernenti i dati trattati ai sensi del presente regolamento; le misure transitorie che saranno necessarie; le disposizioni relative ai costi derivanti dal presente regolamento; gli obblighi riguardanti le comunicazioni; l'entrata in funzione delle misure proposte nel presente regolamento; le modalità di gestione, tra cui la costituzione di un comitato e di un gruppo consultivo, la responsabilità di eu-LISA in materia di formazione e un manuale pratico di supporto all'attuazione e alla gestione delle componenti dell'interoperabilità; le procedure relative al monitoraggio e alla valutazione delle misure proposte nel presente regolamento; infine, una disposizione concernente l'entrata in vigore di quest'ultimo.

2017/0352 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (cooperazione giudiziaria e di polizia, asilo e migrazione)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, paragrafo 2, l'articolo 74, l'articolo 78, paragrafo 2, lettera e), l'articolo 79, paragrafo 2, lettera c), l'articolo 82, paragrafo 1, lettera d), l'articolo 85, paragrafo 1, l'articolo 87, paragrafo 2, lettera a), e l'articolo 88, paragrafo 2,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

sentito il garante europeo della protezione dei dati,

visto il parere del Comitato economico e sociale europeo[43],

visto il parere del Comitato delle regioni[44],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Nella comunicazione del 6 aprile 2016 dal titolo *Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza*[45], la Commissione ha sottolineato la necessità di migliorare l'architettura di gestione dei dati dell'Unione per la gestione delle frontiere e la sicurezza. La comunicazione ha dato il via ad un processo mirante alla realizzazione dell'interoperabilità tra i sistemi di informazione dell'UE relativi alla sicurezza, alle frontiere e alla gestione della migrazione, allo scopo di colmare le carenze strutturali di tali sistemi che ostacolano il lavoro delle autorità nazionali, garantendo nel contempo che le guardie di frontiera, le autorità doganali, gli operatori di polizia e le autorità giudiziarie dispongano delle informazioni necessarie.

(2) Nella tabella di marcia per rafforzare lo scambio e la gestione di informazioni, comprese soluzioni di interoperabilità nel settore "Giustizia e affari interni" del 6 giugno 2016[46], il Consiglio ha individuato una serie di sfide giuridiche, tecniche e operative riguardanti l'interoperabilità dei sistemi di informazione dell'UE e ha sollecitato la ricerca di soluzioni.

[43] GU C […] del […], pag. […].

[44]

[45] COM(2016) 205 del 6.4.2016.

[46] Tabella di marcia per rafforzare lo scambio e la gestione di informazioni, comprese soluzioni di interoperabilità nel settore "Giustizia e affari interni" — documento del Consiglio 9368/1/16 REV 1, del 6 giugno 2016.

(3) Nella risoluzione del 6 luglio 2016 sulle priorità strategiche per il programma di lavoro della Commissione per il 2017[47], il Parlamento europeo ha chiesto proposte intese a migliorare e sviluppare i sistemi di informazione dell'UE esistenti, far fronte alla carenza di informazioni e progredire verso l'interoperabilità, nonché proposte concernenti lo scambio obbligatorio di informazioni a livello dell'UE, assicurando nel contempo le necessarie garanzie in materia di protezione dei dati.

(4) Il Consiglio europeo del 15 dicembre 2016[48] ha sollecitato il conseguimento di ulteriori risultati sull'interoperabilità dei sistemi di informazione e delle banche dati dell'UE.

(5) Nella relazione finale dell'11 maggio 2017[49], il gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità ha concluso che era necessario e tecnicamente fattibile adoperarsi per giungere a soluzioni pratiche in materia di interoperabilità e che tali soluzioni, in linea di massima, potevano offrire vantaggi operativi ed essere introdotte nel rispetto dei requisiti in materia di protezione dei dati.

(6) Nella comunicazione del 16 maggio 2017 contenente la *Settima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza*[50], la Commissione, in linea con quanto esposto nella comunicazione del 6 aprile 2016 e confermato dai risultati e dalle raccomandazioni del gruppo ad alto livello sui sistemi di informazione e l'interoperabilità, ha delineato un nuovo approccio alla gestione dei dati relativi alle frontiere, alla sicurezza e alla migrazione, in base al quale tutti i sistemi di informazione dell'UE per la gestione della sicurezza, delle frontiere e della migrazione sono interoperabili, nel pieno rispetto dei diritti fondamentali.

(7) Nelle conclusioni del 9 giugno 2017 sulla via da seguire per migliorare lo scambio di informazioni e garantire l'interoperabilità dei sistemi d'informazione dell'UE[51], il Consiglio ha invitato la Commissione a portare avanti le soluzioni di interoperabilità proposte dal gruppo di esperti ad alto livello.

(8) Il Consiglio europeo del 23 giugno 2017[52] ha sottolineato la necessità di migliorare l'interoperabilità fra le banche dati e ha invitato la Commissione ad elaborare quanto prima un progetto di normativa che desse attuazione alle proposte formulate dal gruppo di esperti di alto livello sui sistemi di informazione e l'interoperabilità.

(9) Per migliorare la gestione delle frontiere esterne, contribuire a prevenire e contrastare la migrazione irregolare e concorrere a garantire un alto livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, inclusi il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri, è opportuno rendere interoperabili i sistemi di informazione dell'UE, segnatamente il sistema di ingressi/uscite (EES), il sistema di informazione visti (VIS), [il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)], l'Eurodac, il sistema d'informazione Schengen (SIS) e il [sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (sistema ECRIS-TCN)], affinché essi si integrino reciprocamente unitamente ai relativi dati. A tal fine è opportuno istituire un portale di ricerca europeo (ESP), un

---

47 Risoluzione del Parlamento europeo del 6 luglio 2016 sulle priorità strategiche per il programma di lavoro della Commissione per il 2017 [2016/2773 (RSP)].

48 http://www.consilium.europa.eu/media/21917/15-euco-conclusions-final-it.pdf.

49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

50 COM(2017) 261 final del 16.5.2017.

51 http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf.

52 Conclusioni del Consiglio europeo del 22 e 23 giugno 2017.

servizio comune di confronto biometrico (BMS comune), un archivio comune di dati di identità (CIR) e un rilevatore di identità multiple (MID) che fungano da componenti dell'interoperabilità.

(10) L'interoperabilità dovrebbe consentire ai sistemi di informazione dell'UE di integrarsi reciprocamente al fine di facilitare la corretta identificazione delle persone, contribuire alla lotta contro la frode di identità, migliorare e uniformare i requisiti in materia di qualità dei dati dei rispettivi sistemi di informazione dell'UE, agevolare l'attuazione tecnica e operativa dei sistemi di informazione dell'UE attuali e futuri da parte degli Stati membri, rafforzare e semplificare le garanzie in materia di sicurezza e protezione dei dati che presiedono ai rispettivi sistemi di informazione dell'UE, razionalizzare l'accesso all'EES, al VIS, all'[ETIAS] e all'Eurodac a fini di contrasto e sostenere le finalità dell'EES, del VIS, dell'[ETIAS], dell'Eurodac, del SIS e del [sistema ECRIS-TCN].

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

(12) Le componenti dell'interoperabilità dovrebbero riguardare le persone i cui dati personali possono essere trattati nell'ambito dei sistemi di informazione dell'UE e da Europol, vale a dire i cittadini di paesi terzi i cui dati personali sono trattati nell'ambito dei sistemi di informazione dell'UE e da Europol e i cittadini dell'UE i cui dati personali sono trattati nell'ambito del SIS e da Europol.

(13) È opportuno istituire un portale di ricerca europeo (ESP) al fine di facilitare, dal punto di vista tecnico, l'accesso delle autorità degli Stati membri e degli organi dell'UE, in modo rapido, continuato, efficace, sistematico e controllato, ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol, di cui hanno bisogno per svolgere i loro compiti, conformemente ai rispettivi diritti di accesso, e di sostenere gli obiettivi dell'EES, del VIS, [dell'ETIAS], dell'Eurodac, del SIS, [del sistema ECRIS-TCN] e dei dati Europol. Permettendo l'interrogazione simultanea e parallela di tutti i sistemi di informazione dell'UE pertinenti, nonché dei dati Europol e delle banche dati Interpol, l'ESP dovrebbe fungere da interfaccia unica o da mediatore di messaggi ("message broker") per la consultazione di diversi sistemi centrali e per il recupero agevole delle informazioni necessarie, nel pieno rispetto dei requisiti concernenti il controllo degli accessi e la protezione dei dati dei sistemi sottostanti.

(14) Gli utenti finali del portale di ricerca europeo (ESP) che hanno il diritto di accedere ai dati Europol a norma del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio[53] dovrebbero poter consultare i dati Europol simultaneamente ai sistemi di informazione dell'UE ai quali hanno accesso. Qualsiasi ulteriore trattamento dei dati successivo a tale consultazione dovrebbe avvenire a norma del regolamento (UE) 2016/794, comprese le limitazioni all'accesso o all'uso imposte dal fornitore dei dati.

(15) Il portale di ricerca europeo (ESP) dovrebbe essere sviluppato e configurato in modo tale da non consentire, per le interrogazioni, l'uso di campi di dati non riguardanti persone o documenti di viaggio o non presenti in un sistema di informazione dell'UE, nei dati Europol o nella banca dati Interpol.

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

(16) Per garantire l'utilizzo rapido e sistematico di tutti i sistemi di informazione dell'UE, il portale di ricerca europeo (ESP) dovrebbe essere usato per interrogare l'archivio comune di dati di identità, l'EES, il VIS, l'[ETIAS], l'Eurodac e [il sistema ECRIS-TCN]. Il collegamento nazionale ai diversi sistemi di informazione dell'UE dovrebbe comunque essere mantenuto, così da offrire la possibilità di ricorrere tecnicamente a una procedura sostitutiva. L'ESP dovrebbe inoltre essere utilizzato dagli organi dell'Unione per interrogare il SIS centrale conformemente ai rispettivi diritti di accesso e ai fini dell'espletamento dei loro compiti. Esso dovrebbe essere un mezzo supplementare per interrogare il SIS centrale, i dati Europol e i sistemi Interpol, integrando le interfacce specifiche esistenti.

(17) Essendo unici, i dati biometrici quali le impronte digitali e le immagini del volto sono molto più attendibili dei dati alfanumerici per l'identificazione di una persona. Il servizio comune di confronto biometrico (BMS comune) dovrebbe essere uno strumento tecnico da utilizzare per rafforzare e agevolare il lavoro dei sistemi di informazione dell'UE pertinenti e delle altre componenti dell'interoperabilità. Dovrebbe avere principalmente lo scopo di facilitare l'identificazione di una persona che può essere registrata in più banche dati, confrontando i dati biometrici contenuti nei vari sistemi e avvalendosi di una sola componente tecnologica, invece che di cinque diverse, una per ciascuno dei sistemi sottostanti. Avvalendosi di un'unica e non di tante componenti tecnologiche diverse, una per ciascuno dei sistemi sottostanti, il BMS comune dovrebbe contribuire alla sicurezza e offrire vantaggi in termini finanziari, operativi e di manutenzione. Tutti i sistemi automatizzati di identificazione dattiloscopica, inclusi quelli attualmente utilizzati per l'Eurodac, il VIS e il SIS, usano template biometrici costituiti da dati ricavati mediante estrazione di parametri di campioni biometrici effettivi. Il BMS comune dovrebbe riunire e conservare tutti i template biometrici in un unico luogo, facilitando il confronto trasversale ai vari sistemi mediante l'uso di dati biometrici e permettendo economie di scala nello sviluppo e nella manutenzione dei sistemi centrali dell'UE.

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

(19) Per essere efficaci, i sistemi istituiti dal regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio[54], dal regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio[55] e dal [regolamento ETIAS] per la gestione delle frontiere dell'Unione, il sistema istituito dal [regolamento Eurodac] per identificare i richiedenti protezione internazionale e contrastare la migrazione irregolare e il sistema istituito dal [regolamento ECRIS-TCN] devono basarsi sull'identificazione precisa dei cittadini di paesi terzi di cui conservano i dati personali.

---

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

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

(20) L'archivio comune di dati di identità (CIR) dovrebbe pertanto agevolare e contribuire alla corretta identificazione delle persone registrate nell'EES, nel VIS, nell'[ETIAS], nell'Eurodac e nel [sistema ECRIS-TCN].

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

(22) La nuova operazione di trattamento consistente nel conservare questo tipo di dati nell'archivio comune di dati di identità (CIR) anziché in ciascun sistema separato è necessaria per migliorare l'accuratezza dell'identificazione, resa possibile grazie al confronto e all'abbinamento automatizzati dei dati stessi. Il fatto che i dati biometrici e di identità dei cittadini di paesi terzi siano conservati nel CIR non dovrebbe ostacolare in alcun modo il trattamento dei dati ai fini dei regolamenti EES, VIS, ETIAS, Eurodac o ECRIS-TCN, poiché il CIR dovrebbe essere una nuova componente comune di tali sistemi sottostanti.

(23) A questo proposito, la creazione di un fascicolo individuale nell'archivio comune di dati di identità (CIR) per ogni persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nel sistema ECRIS-TCN è necessaria ai fini di una corretta identificazione dei cittadini di paesi terzi all'interno dello spazio Schengen e quale supporto al funzionamento del rilevatore di identità multiple, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. Il fascicolo individuale dovrebbe conservare in un unico luogo tutte le possibili identità connesse a una data persona e renderle accessibili agli utenti finali debitamente autorizzati.

(24) L'archivio comune di dati di identità (CIR) dovrebbe pertanto fungere da supporto al funzionamento del rilevatore di identità multiple e agevolare e semplificare l'accesso delle autorità di contrasto ai sistemi di informazione dell'UE che non sono istituiti esclusivamente a fini di prevenzione, indagine, accertamento o perseguimento di reati gravi.

(25) L'archivio comune di dati di identità (CIR) dovrebbe offrire un contenitore comune per i dati biometrici e di identità dei cittadini di paesi terzi registrati nell'EES, nel VIS, nell'[ETIAS], nell'Eurodac e nel [sistema ECRIS-TCN], che funga da componente comune a questi sistemi ai fini della conservazione di tali dati, e consentirne l'interrogazione.

(26) Tutte le registrazioni nell'archivio comune di dati di identità (CIR) dovrebbero essere separate logicamente mediante l'apposizione automatica, su ciascuna di esse, di un'etichetta che indichi il sistema sottostante da cui provengono. Il sistema di

controllo degli accessi del CIR dovrebbe utilizzare queste etichette per permettere o meno l'accesso alle registrazioni.

(27) Per garantire la corretta identificazione di una persona, le autorità degli Stati membri responsabili della prevenzione e del contrasto della migrazione irregolare e le autorità competenti ai sensi dell'articolo 3, punto 7, della direttiva 2016/680 dovrebbero essere autorizzate ad interrogare l'archivio comune di dati di identità (CIR) usando i dati biometrici di tale persona raccolti durante una verifica di identità.

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

(29) Gli Stati membri dovrebbero adottare misure legislative nazionali per designare le autorità competenti a svolgere le verifiche di identità mediante l'uso dell'archivio comune di dati di identità (CIR) e stabilire le procedure, le condizioni e i criteri di queste verifiche, nel rispetto del principio di proporzionalità. Dette misure, in particolare, dovrebbero conferire a tali autorità il potere di raccogliere dati biometrici della persona durante una verifica di identità effettuata in presenza di un loro rappresentante.

(30) Il presente regolamento dovrebbe dare alle autorità di contrasto designate dallo Stato membro e a Europol una nuova possibilità di accesso semplificato ad altri dati rispetto a quelli di identità presenti nell'EES, nel VIS, nell'[ETIAS] o nell'Eurodac. I dati, compresi dati diversi da quelli di identità contenuti in tali sistemi, possono essere necessari, in casi specifici, a fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo o altri reati gravi.

(31) Il pieno accesso ai dati contenuti nei sistemi di informazione dell'UE necessari a fini di prevenzione, accertamento e indagine di reati di terrorismo o di altri reati gravi, diversi dai dati di identità pertinenti contenuti nell'archivio comune di dati di identità (CIR) ottenuti utilizzando i dati biometrici dell'interessato raccolti nel corso di una verifica di identità, dovrebbe continuare ad essere disciplinato dalle disposizioni dei rispettivi strumenti giuridici. Le autorità di contrasto designate ed Europol non sanno in anticipo quale sistema di informazione dell'UE contenga dati sulle persone su cui devono compiere indagini. Ciò causa ritardi e inefficienze nell'espletamento delle loro mansioni. Di conseguenza, l'utente finale autorizzato dall'autorità designata dovrebbe avere la facoltà di vedere in quale sistema di informazione dell'UE sono registrati i dati corrispondenti all'interrogazione effettuata. Il sistema interessato verrebbe quindi segnalato in esito alla verifica automatica della presenza di un riscontro positivo nel sistema (la cosiddetta funzione di segnalazione "hit/no hit").

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

(33) Per dar modo alle autorità designate dello Stato membro e ad Europol di interrogare l'archivio comune di dati di identità (CIR) al fine di ottenere un riscontro che segnali la presenza o meno di dati nell'EES, nel VIS, [nell'ETIAS] o nell'Eurodac, è necessario il trattamento automatizzato dei dati personali. La segnalazione del riscontro positivo non rivelerebbe i dati personali dell'interessato, ma si limiterebbe ad indicare che alcuni dei suoi dati sono conservati in uno dei sistemi. L'utente finale autorizzato non dovrebbe assumere alcuna decisione sfavorevole all'interessato basandosi unicamente sulla semplice segnalazione di un riscontro positivo. L'accesso dell'utente finale a tale segnalazione costituirebbe pertanto un'ingerenza molto limitata nel diritto alla protezione dei dati personali dell'interessato, mentre sarebbe necessario per consentire all'autorità designata e ad Europol di inoltrare in modo più efficace la richiesta di accesso ai dati personali direttamente al sistema che, secondo quanto indicato dalla segnalazione, li contiene.

(34) Le due fasi di consultazione dei dati risultano particolarmente efficaci qualora l'autore presunto o effettivo oppure la vittima presunta di un reato di terrorismo o di un altro reato grave sia sconosciuto/sconosciuta. In questi casi l'archivio comune di dati di identità (CIR) dovrebbe permettere di identificare, con un'unica ricerca, il sistema di informazione che conosce la persona. Con l'introduzione dell'obbligo di utilizzare, in casi del genere, questo nuovo approccio per l'accesso a fini di contrasto, l'accesso ai dati personali conservati nell'EES, nel VIS, nell'[ETIAS] e nell'Eurodac dovrebbe aver luogo senza che occorra effettuare preventivamente una ricerca nelle banche dati nazionali o avviare una ricerca preliminare nel sistema automatizzato di identificazione dattiloscopica di altri Stati membri ai sensi della decisione 2008/615/GAI. Il principio della ricerca preliminare, in effetti, limita la possibilità delle autorità degli Stati membri di consultare i sistemi per finalità di contrasto giustificate e, quindi, potrebbe tradursi nella mancata opportunità di scoprire le informazioni necessarie. L'obbligo di effettuare preventivamente una ricerca nelle banche dati nazionali e di avviare una ricerca preliminare nel sistema automatizzato di identificazione dattiloscopica di altri Stati membri ai sensi della decisione 2008/615/GAI dovrebbe cessare di applicarsi solo dopo che sia diventata operativa la garanzia alternativa dell'approccio in due fasi per l'accesso a fini di contrasto mediante il CIR.

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

(36) Il conseguimento degli obiettivi dei sistemi di informazione dell'UE è ostacolato dall'attuale impossibilità delle autorità che li utilizzano di effettuare verifiche sufficientemente affidabili dell'identità dei cittadini di paesi terzi i cui dati sono conservati in sistemi diversi. Tale impossibilità deriva dal fatto che un singolo sistema può contenere un insieme di dati di identità fraudolenti, inesatti o incompleti che, ad oggi, non sono assolutamente rilevabili mediante un confronto con i dati conservati in un altro sistema. Per rimediare a questa situazione è necessario dotarsi, a livello dell'Unione, di uno strumento tecnico che consenta un'identificazione precisa dei cittadini di paesi terzi per tali scopi.

(37) Il rilevatore di identità multiple (MID) dovrebbe creare e conservare i collegamenti tra i dati presenti nei vari sistemi di informazione dell'UE ai fini dell'individuazione di

identità multiple, al duplice scopo di agevolare le verifiche di identità per i viaggiatori in buona fede e di contrastare la frode di identità. Il MID dovrebbe contenere solo i collegamenti tra le persone fisiche presenti in più di un sistema di informazione dell'UE, limitandosi rigorosamente ai dati necessari per verificare se l'interessato è registrato lecitamente o illecitamente con identità anagrafiche diverse in sistemi diversi, ovvero per chiarire che due persone aventi dati anagrafici simili possono non essere la stessa persona. Il trattamento dei dati mediante il portale di ricerca europeo (ESP) e il servizio comune di confronto biometrico (BMS comune) al fine di collegare i fascicoli individuali trasversalmente ai singoli sistemi dovrebbe limitarsi al minimo indispensabile e, pertanto, dovrebbe portare alla semplice rilevazione di un'identità multipla nel momento in cui vengono aggiunti nuovi dati a uno dei sistemi di informazione inclusi nell'archivio comune di dati di identità e nel SIS. Il MID dovrebbe prevedere misure di salvaguardia che tutelino le persone con identità multiple lecite da eventuali discriminazioni o decisioni sfavorevoli.

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

(39) Quando un'autorità nazionale o un organo dell'UE crea nuove registrazioni, il portale di ricerca europeo (ESP) e il servizio comune di confronto biometrico (BMS comune) dovrebbero confrontare i dati riguardanti le persone contenuti nell'archivio comune di dati di identità (CIR) e nel SIS. Tale confronto dovrebbe essere automatizzato. Il CIR e il SIS dovrebbero utilizzare il BMS comune per individuare eventuali collegamenti sulla base dei dati biometrici. Dovrebbero utilizzare l'ESP per individuare eventuali collegamenti sulla base dei dati alfanumerici. Dovrebbero infine essere in grado di individuare i dati identici o simili concernenti un cittadino di paese terzo conservati in più sistemi. In tal caso dovrebbe essere creato un collegamento che indichi che si tratta della stessa persona. Il CIR e il SIS dovrebbero essere configurati in modo tale da individuare i piccoli errori di ortografia o di traslitterazione, così da non creare ostacoli ingiustificati al cittadino di paese terzo interessato.

(40) L'autorità nazionale o l'organo dell'UE che ha registrato i dati nel sistema di informazione dell'UE pertinente dovrebbe confermare o modificare i suddetti collegamenti. Tale autorità dovrebbe avere accesso ai dati conservati nell'archivio comune di dati di identità (CIR) o nel SIS e nel rilevatore di identità multiple (MID) ai fini della verifica manuale dell'identità.

(41) Le autorità degli Stati membri e gli organi dell'UE che hanno accesso ad almeno un sistema di informazione dell'UE incluso nell'archivio comune di dati di identità (CIR) o al SIS dovrebbero accedere al rilevatore di identità multiple (MID) limitatamente ai cosiddetti collegamenti rossi, vale a dire nel caso in cui i dati oggetto del collegamento presentino gli stessi dati biometrici ma dati di identità differenti e l'autorità responsabile della verifica delle identità diverse abbia concluso che essi si riferiscono alla stessa persona che usa illecitamente le identità in questione, ovvero nel caso in cui i dati oggetto del collegamento presentino dati di identità simili e l'autorità responsabile della verifica delle identità diverse abbia concluso che essi si riferiscono

alla stessa persona che usa illecitamente le identità in questione. Se i dati di identità oggetto del collegamento non sono simili, dovrebbe crearsi un collegamento giallo e si dovrebbe procedere a una verifica manuale che confermi il collegamento o ne modifichi opportunamente il colore.

(42) La verifica manuale delle identità multiple dovrebbe competere all'autorità che ha creato o aggiornato i dati per i quali è emerso un riscontro positivo, che a sua volta ha dato luogo ad un collegamento con i dati già conservati in un altro sistema di informazione dell'UE. L'autorità responsabile della verifica delle identità multiple dovrebbe accertare se esistano più identità, lecite o illecite. Tale accertamento dovrebbe aver luogo, se possibile, in presenza del cittadino di paese terzo, se del caso chiedendo ulteriori chiarimenti o informazioni. Dovrebbe essere effettuato senza indugio, nel rispetto dei requisiti giuridici riguardanti l'accuratezza delle informazioni ai sensi del diritto nazionale e dell'Unione.

(43) Per i collegamenti ottenuti nell'ambito del sistema d'informazione Schengen (SIS) relativamente a segnalazioni di persone ricercate per l'arresto a fini di consegna o di estradizione, di persone scomparse o vulnerabili, di persone ricercate per presenziare ad un procedimento giudiziario, di persone da sottoporre a controllo discreto o a controllo specifico o di ignoti ricercati, l'autorità responsabile della verifica delle identità multiple dovrebbe essere l'ufficio SIRENE dello Stato membro che ha creato la segnalazione. In realtà tali categorie di segnalazioni SIS sono sensibili e non dovrebbero essere necessariamente condivise con le autorità che inseriscono o aggiornano i dati in uno degli altri sistemi di informazione dell'UE. La creazione di un collegamento con i dati del SIS dovrebbe lasciare impregiudicate le azioni da intraprendere a norma dei [regolamenti SIS].

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

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

(46) Il formato universale dei messaggi (UMF) dovrebbe stabilire uno standard per lo scambio strutturato delle informazioni a livello transfrontaliero tra i sistemi di informazione, le autorità e/o le organizzazioni del settore Giustizia e affari interni. Per le informazioni scambiate abitualmente, l'UMF dovrebbe definire un lessico comune e

strutture logiche che facilitino l'interoperabilità permettendo la creazione e la lettura del contenuto dello scambio in modo coerente e semanticamente equivalente.

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

(48) Il regolamento (UE) 2016/679 dovrebbe applicarsi al trattamento dei dati personali nell'ambito del presente regolamento da parte delle autorità nazionali, a meno che tale trattamento non sia effettuato dalle autorità designate o dai punti di accesso centrale degli Stati membri a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, nel qual caso dovrebbe applicarsi la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio.

(49) Le disposizioni specifiche sulla protezione dei dati di cui [al regolamento Eurodac], [al regolamento sul SIS nel settore dell'attività di contrasto], [al regolamento sul SIS nel settore del rimpatrio] e [al regolamento ECRIS-TCN] dovrebbero applicarsi al trattamento dei dati personali nei rispettivi sistemi.

(50) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio[56] dovrebbe applicarsi al trattamento dei dati personali da parte di eu-LISA e di altre istituzioni e organi dell'Unione nell'assolvimento delle loro responsabilità a norma del presente regolamento, fatto salvo il regolamento (UE) 2016/794, che dovrebbe applicarsi al trattamento dei dati personali da parte di Europol.

(51) Le autorità nazionali di controllo istituite in virtù del [regolamento (UE) 2016/679] dovrebbero verificare la legittimità del trattamento dei dati personali da parte degli Stati membri, mentre il garante europeo della protezione dei dati istituito dal regolamento (CE) n. 45/2001 dovrebbe sorvegliare le attività delle istituzioni e degli organismi dell'Unione connesse al trattamento dei dati personali. Il garante europeo della protezione dei dati e le autorità di controllo dovrebbero collaborare nel sorvegliare il trattamento dei dati personali da parte delle componenti dell'interoperabilità.

(52) "(...) Il garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso un parere il …".

(53) Per quanto riguarda la riservatezza, le disposizioni pertinenti dello statuto dei funzionari e del regime applicabile agli altri agenti dell'Unione europea dovrebbero applicarsi ai funzionari o altri agenti che sono impiegati e che lavorano per il SIS.

[56] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

(54) Sia gli Stati membri che eu-LISA dovrebbero dotarsi di piani di sicurezza che agevolino l'adempimento degli obblighi in tal senso e dovrebbero collaborare per poter risolvere le questioni relative alla sicurezza. eu-LISA dovrebbe inoltre assicurare l'uso continuo dei più recenti sviluppi tecnologici, al fine di garantire l'integrità dei dati per quanto riguarda lo sviluppo, la progettazione e la gestione delle componenti dell'interoperabilità.

(55) A sostegno dell'elaborazione di statistiche e relazioni, è necessario concedere al personale autorizzato delle autorità competenti, delle istituzioni e degli organi di cui al presente regolamento l'accesso alla consultazione di taluni dati relativi a determinate componenti dell'interoperabilità, senza permettere l'identificazione della persona interessata.

(56) Per consentire alle autorità competenti e agli organi dell'UE di adeguarsi ai nuovi requisiti relativi all'uso del portale di ricerca europeo (ESP) è necessario prevedere un periodo transitorio. Analogamente, dovrebbero essere stabilite misure transitorie per l'entrata in funzione del rilevatore di identità multiple (MID), al fine di consentirne un funzionamento coerente e ottimale.

(57) I costi per lo sviluppo delle componenti dell'interoperabilità previsti nell'ambito dell'attuale quadro finanziario pluriennale sono inferiori all'importo rimanente della dotazione di bilancio destinata alle "frontiere intelligenti" di cui al regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio[57]. Di conseguenza, ai sensi dell'articolo 5, paragrafo 5, lettera b), del regolamento (UE) n. 515/2014, il presente regolamento dovrebbe riassegnare l'importo attualmente destinato allo sviluppo di sistemi informatici a sostegno della gestione dei flussi migratori attraverso le frontiere esterne.

(58) Al fine di integrare alcuni aspetti tecnici dettagliati del presente regolamento, è opportuno delegare alla Commissione il potere di adottare atti in conformità dell'articolo 290 del trattato sul funzionamento dell'Unione europea che riguardino i profili degli utenti del portale di ricerca europeo (ESP) e il contenuto e il formato delle risposte di tale portale. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[58]. In particolare, al fine di garantire una partecipazione paritaria alla preparazione degli atti delegati, è opportuno che il Parlamento europeo e il Consiglio ricevano l'intera documentazione contemporaneamente agli esperti degli Stati membri e che i loro esperti abbiano sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti.

(59) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione per l'adozione di norme dettagliate riguardanti: meccanismi, procedure e indicatori automatizzati di controllo della qualità dei dati, lo sviluppo dello standard UMF, le procedure per determinare i casi di identità simili, il funzionamento dell'archivio centrale di relazioni e statistiche e la procedura di cooperazione in caso di incidenti di sicurezza. È

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

[58] http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv%3AOJ.L_.2016.123.01.0001.01.ITA

opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[59].

(60) Il regolamento (UE) 2016/794 si applica a qualunque trattamento dei dati Europol ai fini del presente regolamento.

(61) Il presente regolamento non pregiudica l'applicazione della direttiva 2004/38/CE.

(62) In conformità dell'articolo 3 dell'accordo tra la Comunità europea e il Regno di Danimarca in merito ai criteri e ai meccanismi di determinazione dello Stato competente per l'esame di una domanda d'asilo presentata in Danimarca oppure in uno degli altri Stati membri dell'Unione europea e in merito a "Eurodac" per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino[60], la Danimarca deve notificare alla Commissione se intende o meno attuare il contenuto del presente regolamento nella misura in cui riguarda l'Eurodac [e il sistema automatizzato per la registrazione, il monitoraggio e il meccanismo di assegnazione delle domande di protezione internazionale di cui all'articolo 44 del regolamento (UE) XX/XX 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 (rifusione)].

(63) Nella misura in cui le disposizioni riguardano il SIS quale disciplinato dalla decisione 2007/533/GAI, il Regno Unito partecipa al presente regolamento ai sensi dell'articolo 5, paragrafo 1, del protocollo n. 19 sull'*acquis* di Schengen integrato nell'ambito dell'Unione europea, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea ("protocollo sull'*acquis* di Schengen"), e dell'articolo 8, paragrafo 2, della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'*acquis* di Schengen[61]. Inoltre, nella misura in cui le disposizioni riguardano l'Eurodac [e il sistema automatizzato per la registrazione, il monitoraggio e il meccanismo di assegnazione delle domande di protezione internazionale di cui all'articolo 44 del regolamento (UE) XX/XX 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 (rifusione)], il Regno Unito può notificare al presidente del Consiglio che desidera partecipare all'adozione e all'applicazione del presente regolamento, 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 trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea ("protocollo sulla posizione del Regno Unito e dell'Irlanda"). Nella misura in cui le disposizioni riguardano il [sistema ECRIS-TCN], a norma degli articoli 1 e 2, nonché dell'articolo 4 bis, paragrafo 1, del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, il Regno Unito non partecipa all'adozione del presente regolamento, non è da esso vincolato né è soggetto alla sua applicazione. A norma dell'articolo 3 e dell'articolo 4 bis, paragrafo 1, del protocollo n. 21, il Regno Unito può notificare che desidera partecipare all'adozione del presente regolamento.

---

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

[60]

[61]

(64) Nella misura in cui le disposizioni riguardano il SIS II quale disciplinato dalla decisione 2007/533/GAI, l'Irlanda partecipa al presente regolamento ai sensi dell'articolo 5, paragrafo 1, del protocollo n. 19 sull'*acquis* di Schengen integrato nell'ambito dell'Unione europea, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea ("protocollo sull'*acquis* di Schengen"), e dell'articolo 6, paragrafo 2, della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'*acquis* di Schengen[62]. Inoltre, nella misura in cui le disposizioni riguardano l'Eurodac [e il sistema automatizzato per la registrazione, il monitoraggio e il meccanismo di assegnazione delle domande di protezione internazionale di cui all'articolo 44 del regolamento (UE) XX/XX 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 (rifusione)], l'Irlanda può notificare al presidente del Consiglio che desidera partecipare all'adozione e all'applicazione del presente regolamento, 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 trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea ("protocollo sulla posizione del Regno Unito e dell'Irlanda"). Nella misura in cui le disposizioni riguardano il [sistema ECRIS-TCN], a norma degli articoli 1 e 2, nonché dell'articolo 4 bis, paragrafo 1, del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, l'Irlanda non partecipa all'adozione del presente regolamento, non è da esso vincolata né è soggetta alla sua applicazione. A norma dell'articolo 3 e dell'articolo 4 bis, paragrafo 1, del protocollo n. 21, l'Irlanda può notificare che desidera partecipare all'adozione del presente regolamento.

(65) Per quanto riguarda l'Islanda e la Norvegia, relativamente all'Eurodac [e al sistema automatizzato per la registrazione, il monitoraggio e il meccanismo di assegnazione delle domande di protezione internazionale di cui all'articolo 44 del regolamento (UE) XX/XX 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 (rifusione)], il presente regolamento costituisce una nuova misura ai sensi dell'accordo tra la Comunità europea e la Repubblica d'Islanda e il Regno di Norvegia relativo ai criteri e ai meccanismi per determinare lo Stato competente per l'esame di una domanda d'asilo presentata in uno Stato membro oppure in Islanda o in Norvegia.

(66) Per quanto riguarda la Svizzera, relativamente all'Eurodac [e al sistema automatizzato per la registrazione, il monitoraggio e il meccanismo di assegnazione delle domande di protezione internazionale di cui all'articolo 44 del regolamento (UE) XX/XX 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 (rifusione)], il presente regolamento costituisce una nuova misura riguardante l'Eurodac ai sensi dell'accordo tra la Comunità europea e la Confederazione svizzera relativo ai criteri e ai meccanismi che permettono di determinare lo Stato competente per l'esame di una domanda di asilo introdotta in uno degli Stati membri o in Svizzera.

62

(67) Per quanto riguarda il Liechtenstein, relativamente all'Eurodac [e al sistema automatizzato per la registrazione, il monitoraggio e il meccanismo di assegnazione delle domande di protezione internazionale di cui all'articolo 44 del regolamento (UE) XX/XX 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 (rifusione)], il presente regolamento costituisce una nuova misura ai sensi del protocollo sottoscritto tra la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'accordo tra la Comunità europea e la Confederazione svizzera relativo ai criteri e ai meccanismi che permettono di determinare lo Stato competente per l'esame di una domanda di asilo introdotta in uno degli Stati membri o in Svizzera.

(68) Il presente regolamento rispetta i diritti fondamentali ed osserva i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea ed è applicato conformemente a tali diritti e principi,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I
Disposizioni generali

Articolo 1
Oggetto

1. Il presente regolamento, unitamente al [regolamento 2018/xx sull'interoperabilità in materia di frontiere e visti], istituisce un quadro per garantire l'interoperabilità tra il sistema di ingressi/uscite (EES), il sistema di informazione visti (VIS), [il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)], l'Eurodac, il sistema d'informazione Schengen (SIS) e [il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (sistema ECRIS-TCN)] affinché tali sistemi e dati si integrino reciprocamente.

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

   (a) un portale di ricerca europeo (ESP);

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

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

   (d) un rilevatore di identità multiple (MID).

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

4. Il presente regolamento adatta le procedure e le condizioni per l'accesso delle autorità di contrasto degli Stati membri e dell'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) all'EES, al VIS, [all'ETIAS] e

all'Eurodac a fini di prevenzione, accertamento e indagine di reati di terrorismo o altri reati gravi di loro competenza.

Articolo 2
Obiettivi dell'interoperabilità

1. Garantendo l'interoperabilità il presente regolamento persegue i seguenti obiettivi:
   (a) migliorare la gestione delle frontiere esterne;
   (b) contribuire a prevenire e combattere l'immigrazione irregolare;
   (c) contribuire ad assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, inclusi il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri;
   (d) migliorare l'attuazione della politica comune in materia di visti;
   (e) aiutare a esaminare le domande di protezione internazionale.
2. Gli obiettivi dell'interoperabilità sono realizzati:
   (a) garantendo la corretta identificazione delle persone;
   (b) contribuendo a contrastare la frode di identità;
   (c) migliorando e armonizzando i requisiti di qualità dei dati dei diversi sistemi di informazione dell'UE;
   (d) agevolando gli Stati membri nell'attuazione tecnica e operativa degli attuali e futuri sistemi di informazione dell'UE;
   (e) rafforzando, semplificando e rendendo più uniformi le condizioni di sicurezza e protezione dei dati che disciplinano i diversi sistemi di informazione dell'UE;
   (f) semplificando le condizioni di accesso all'EES, al VIS, [all'ETIAS] e all'Eurodac a fini di contrasto;
   (g) sostenendo le finalità dell'EES, del VIS, [dell'ETIAS], dell'Eurodac, del SIS e [del sistema ECRIS-TCN].

Articolo 3
Ambito di applicazione

1. Il presente regolamento si applica all'Eurodac, al SIS e [al sistema ECRIS-TCN].
2. Il presente regolamento si applica ai dati Europol nella misura in cui consente di interrogarli simultaneamente ai sistemi di informazione dell'UE di cui al paragrafo 1 nel rispetto del diritto dell'Unione.
3. Il presente regolamento si applica alle persone i cui dati personali possono essere trattati nei sistemi di informazione dell'UE di cui al paragrafo 1 e nei dati Europol di cui al paragrafo 2.

Articolo 4
Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

(2) “frontiere esterne”: le frontiere esterne quali definite all’articolo 2, punto 2, del regolamento (UE) 2016/399;

(3) “verifiche di frontiera”: le verifiche di frontiera quali definite all’articolo 2, punto 11, del regolamento (UE) 2016/399;

(4) “autorità di frontiera”: le guardie di frontiera incaricate, conformemente al diritto nazionale, di procedere alle verifiche di frontiera;

(5) “autorità di controllo”: l’autorità di controllo istituita in virtù dell’articolo 51, paragrafo 1, del regolamento (UE) 2016/679 e l’autorità di controllo istituita in virtù dell’articolo 41, paragrafo 1, della direttiva (UE) 2016/680;

(6) “verifica”: il procedimento di confronto di serie di dati al fine di verificare la validità di una identità dichiarata (verifica “uno a uno”);

(7) “identificazione”: il procedimento volto a determinare l’identità di una persona mediante interrogazione di una banca dati confrontando varie serie di dati (verifica “uno a molti”);

(8) “cittadino di paese terzo”: chi non è cittadino dell’Unione ai sensi dell’articolo 20, paragrafo 1, del trattato, l’apolide o qualsiasi persona la cui cittadinanza è ignota;

(9) “dati alfanumerici”: i dati rappresentati da lettere, cifre, caratteri speciali, spazi e segni di punteggiatura;

(10) “dati di identità”: i dati di cui all’articolo 27, paragrafo 3, lettere da a) a h);

(11) “dati relativi alle impronte digitali”: i dati sulle impronte digitali di una persona;

(12) “immagine del volto”: le immagini digitalizzate del volto;

(13) “dati biometrici”: i dati relativi alle impronte digitali e/o all’immagine del volto;

(14) “template biometrico”: la rappresentazione matematica ottenuta estraendo elementi dai dati biometrici, limitatamente alle caratteristiche necessarie per effettuare identificazioni e verifiche;

(15) “documento di viaggio”: il passaporto o altro documento equivalente che autorizza il titolare ad attraversare le frontiere esterne e sul quale può essere apposto un visto;

(16) “dati del documento di viaggio”: tipo, numero e paese di rilascio del documento di viaggio, data di scadenza della validità del documento di viaggio e codice a tre lettere del paese di rilascio del documento di viaggio;

(17) “autorizzazione ai viaggi”: l’autorizzazione ai viaggi di cui all’articolo 3 del [regolamento ETIAS];

(18) “visto per soggiorno di breve durata”: il visto quale definito all’articolo 2, punto 2, lettera a), del regolamento (CE) n. 810/2009;

(19) “sistemi di informazione dell’UE”: i sistemi IT su larga scala gestiti da eu-LISA;

(20) “dati Europol”: i dati personali forniti a Europol per la finalità di cui all’articolo 18, paragrafo 2, lettera a), del regolamento (UE) 2016/794;

(21) “banche dati Interpol”: la banca dati Interpol sui documenti di viaggio rubati o smarriti (SLTD) e la banca dati Interpol sui documenti di viaggio associati a segnalazioni (TDAWN);

(22) “corrispondenza”: la coincidenza constatata confrontando due o più occorrenze di dati personali registrati o in fase di registrazione in un sistema di informazione o in una banca dati;

(23) “riscontro positivo”: la conferma di una o più corrispondenze;

(24) “autorità di polizia”: l’autorità competente quale definita all’articolo 3, punto 7, della direttiva (UE) 2016/680;

(25) “autorità designate”: le autorità designate dagli Stati membri, di cui all’articolo 29, paragrafo 1, del regolamento (UE) 2017/2226, all’articolo 3, paragrafo 1, della decisione 2008/633/GAI del Consiglio, [all’articolo 43 del regolamento ETIAS] e [all’articolo 6 del regolamento Eurodac];

(26) “reato di terrorismo”: il reato che, ai sensi del diritto nazionale, corrisponde o è equivalente a uno dei reati di cui alla direttiva (UE) 2017/541;

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

(28) “EES”: il sistema di ingressi/uscite di cui al regolamento (UE) 2017/2226;

(29) “VIS”: il sistema di informazione visti di cui al regolamento (CE) n. 767/2008;

(30) [“ETIAS”: il sistema europeo di informazione e autorizzazione ai viaggi di cui al regolamento ETIAS;]

(31) “Eurodac”: l’Eurodac di cui al [regolamento Eurodac];

(32) “SIS”: il sistema d’informazione Schengen di cui [al regolamento sul SIS nel settore delle verifiche di frontiera, al regolamento sul SIS nel settore dell’attività di contrasto e al regolamento sul SIS nel settore del rimpatrio];

(33) [“sistema ECRIS-TCN”: il sistema europeo di informazione sui casellari giudiziali contenente informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi, di cui al regolamento sul sistema ECRIS-TCN;]

(34) “portale di ricerca europeo”, “portale” o “ESP”: il portale di ricerca europeo di cui all’articolo 6;

(35) “servizio comune di confronto biometrico” o “BMS comune”: il servizio comune di confronto biometrico di cui all’articolo 15;

(36) “archivio comune di dati di identità”, “archivio comune” o “CIR”: l’archivio comune di dati di identità di cui all’articolo 17;

(37) “rilevatore di identità multiple” o “MID”: il rilevatore di identità multiple di cui all’articolo 25;

(38) “archivio centrale di relazioni e statistiche” o “CRRS”: l’archivio centrale di relazioni e statistiche di cui all’articolo 39.

Articolo 5
Non discriminazione

Il trattamento di dati personali ai fini del presente regolamento non dà luogo a discriminazioni nei confronti delle persone fondate sul sesso, sulla razza o sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale. Esso rispetta pienamente la dignità e l'integrità umana. È prestata particolare attenzione ai minori, alle persone anziane e alle persone con disabilità.

CAPO II
Portale di ricerca europeo

Articolo 6
Portale di ricerca europeo

1. È istituito un portale di ricerca europeo (ESP) al fine di permettere alle autorità degli Stati membri e agli organi dell'UE di accedere in modo rapido, continuato, efficace, sistematico e controllato ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol di cui hanno bisogno per svolgere i loro compiti, conformemente ai rispettivi diritti di accesso, e di sostenere gli obiettivi dell'EES, del VIS, [dell'ETIAS], dell'Eurodac, del SIS, [del sistema ECRIS-TCN] e dei dati Europol.
2. Il portale di ricerca europeo è composto di:
   (a) un'infrastruttura centrale, che comprende un portale di ricerca per l'interrogazione simultanea dell'EES, del VIS, [dell'ETIAS], dell'Eurodac, del SIS, [del sistema ECRIS-TCN], dei dati Europol e delle banche dati Interpol;
   (b) un canale di comunicazione sicuro tra il portale di ricerca europeo, gli Stati membri e gli organi dell'UE autorizzati ad usare il portale conformemente al diritto dell'Unione;
   (c) un'infrastruttura di comunicazione sicura tra il portale di ricerca europeo e l'EES, il VIS, [l'ETIAS], l'Eurodac, il SIS centrale, [il sistema ECRIS-TCN], i dati Europol e le banche dati Interpol nonché tra il portale e le infrastrutture centrali dell'archivio comune di dati di identità e del rilevatore di identità multiple.
3. eu-LISA provvede allo sviluppo del portale di ricerca europeo e ne assicura la gestione tecnica.

Articolo 7
Uso del portale di ricerca europeo

1. L'uso del portale di ricerca europeo è riservato alle autorità degli Stati membri e agli organi dell'UE che hanno accesso all'EES, [all'ETIAS], al VIS, al SIS, all'Eurodac, [al sistema ECRIS-TCN], all'archivio comune di dati di identità, al rilevatore di identità multiple, ai dati Europol e alle banche dati Interpol, nel rispetto del diritto dell'Unione o nazionale che disciplina tale accesso.
2. Le autorità di cui al paragrafo 1 usano il portale di ricerca europeo per cercare dati relativi a persone o documenti di viaggio nei sistemi centrali dell'Eurodac e [del sistema ECRIS-TCN], conformemente ai rispettivi diritti di accesso a norma del

diritto dell'Unione e nazionale. Si avvalgono di tale portale anche per interrogare l'archivio comune di dati di identità, conformemente ai rispettivi diritti di accesso a norma del presente regolamento, ai fini degli articoli 20, 21 e 22.

3. Le autorità degli Stati membri di cui al paragrafo 1 possono usare il portale di ricerca europeo per cercare dati relativi a persone o documenti di viaggio nel SIS centrale di cui [al regolamento sul SIS nel settore delle verifiche di frontiera e al regolamento sul SIS nel settore dell'attività di contrasto]. L'accesso al SIS centrale tramite il portale di ricerca europeo è effettuato attraverso il sistema nazionale (N.SIS) di ciascuno Stato membro conformemente [all'articolo 4, paragrafo 2, del regolamento sul SIS nel settore delle verifiche di frontiera e del regolamento sul SIS nel settore dell'attività di contrasto].

4. Gli organi dell'UE usano il portale di ricerca europeo per cercare nel SIS centrale dati relativi a persone o documenti di viaggio.

5. Le autorità di cui al paragrafo 1 possono usare il portale di ricerca europeo per cercare dati relativi a persone o documenti di viaggio nei dati Europol, conformemente ai rispettivi diritti di accesso a norma del diritto dell'Unione e nazionale.

Articolo 8
Profili per gli utenti del portale di ricerca europeo

1. Al fine di consentire l'uso del portale di ricerca europeo, eu-LISA crea per ciascuna categoria di utenti del portale, secondo le modalità tecniche e i diritti di accesso di cui al paragrafo 2, un profilo che comprende, conformemente al diritto dell'Unione e nazionale:

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

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

   (c) i dati forniti in ciascuna risposta.

2. La Commissione adotta atti delegati conformemente all'articolo 63 per specificare le modalità tecniche dei profili di cui al paragrafo 1 per gli utenti del portale di ricerca europeo di cui all'articolo 7, paragrafo 1, nel rispetto dei rispettivi diritti di accesso.

Articolo 9
Interrogazioni

1. Gli utenti del portale di ricerca europeo avviano un'interrogazione inserendo nel portale i dati conformemente ai rispettivi profilo utente e diritti di accesso. Usando i dati così inseriti il portale interroga simultaneamente l'EES, [l'ETIAS], il VIS, il SIS, l'Eurodac, [il sistema ECRIS-TCN], l'archivio comune di dati di identità, i dati Europol e le banche dati Interpol.

2. I campi di dati usati per avviare l'interrogazione tramite il portale di ricerca europeo corrispondono ai campi di dati relativi a persone o documenti di viaggio che possono essere usati per interrogare i vari sistemi di informazione dell'UE, i dati Europol e le banche dati Interpol conformemente agli strumenti giuridici che li disciplinano.

3. eu-LISA implementa un documento di controllo dell'interfaccia per il portale di ricerca europeo basato sul formato universale dei messaggi di cui all'articolo 38.

4. In risposta all'interrogazione del portale l'EES, [l'ETIAS], il VIS, il SIS, l'Eurodac, [il sistema ECRIS-TCN], l'archivio comune di dati di identità, il rilevatore di identità multiple, i dati Europol e le banche dati Interpol forniscono i pertinenti dati in essi contenuti.

5. Il portale di ricerca europeo è progettato in modo da garantire che, quando sono interrogate le banche dati Interpol, i dati usati a tal fine dall'utente del portale non siano condivisi con i proprietari dei dati Interpol.

6. La risposta all'utente del portale è univoca e contiene tutti i dati a cui l'utente ha accesso in base al diritto dell'Unione. Se necessario, la risposta fornita dal portale indica il sistema di informazione o la banca dati cui appartengono i dati.

7. La Commissione adotta un atto delegato conformemente all'articolo 63 per specificare il contenuto e il formato delle risposte del portale di ricerca europeo.

Articolo 10
Registrazioni

1. Fatti salvi [l'articolo 39 del regolamento Eurodac], [gli articoli 12 e 18 del regolamento sul SIS nel settore dell'attività di contrasto], [l'articolo 29 del regolamento ECRIS-TCN] e l'articolo 40 del regolamento (UE) 2016/794, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nel portale di ricerca europeo. Tali registrazioni comprendono, in particolare, i seguenti elementi:

   (a) l'autorità dello Stato membro e il singolo utente del portale di ricerca europeo, compreso il profilo ESP usato di cui all'articolo 8;

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

   (c) i sistemi di informazione dell'UE e i dati Europol interrogati;

   (d) conformemente alle disposizioni nazionali, al regolamento (UE) 2016/794 o, se applicabile, al regolamento (CE) 45/2001, l'identificazione della persona che ha effettuato l'interrogazione.

2. Le registrazioni possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza degli stessi ai sensi dell'articolo 42. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione, a meno che non siano necessarie per procedure di monitoraggio già avviate.

Articolo 11
Procedure sostitutive in caso di impossibilità tecnica dell'uso del portale di ricerca europeo

1. Qualora sia tecnicamente impossibile usare il portale di ricerca europeo per interrogare uno o più sistemi di informazione dell'UE di cui all'articolo 9, paragrafo 1, o l'archivio comune di dati di identità a causa di un guasto del portale, eu-LISA ne informa i relativi utenti.

2. Qualora sia tecnicamente impossibile usare il portale di ricerca europeo per interrogare uno o più sistemi di informazione dell'UE di cui all'articolo 9, paragrafo

1, o l'archivio comune di dati di identità a causa di un guasto dell'infrastruttura nazionale di uno Stato membro, l'autorità competente di tale Stato membro ne informa eu-LISA e la Commissione.

3. In entrambi i casi, fintantoché il guasto tecnico non è riparato l'obbligo di cui all'articolo 7, paragrafi 2 e 4, non si applica e gli Stati membri possono accedere ai sistemi di informazione di cui all'articolo 9, paragrafo 1, o all'archivio comune di dati di identità direttamente tramite le rispettive interfacce uniformi nazionali o le infrastrutture di comunicazione nazionali.

CAPO III
Servizio comune di confronto biometrico

Articolo 12
Servizio comune di confronto biometrico

1. Al fine di sostenere l'archivio comune di dati di identità e il rilevatore di identità multiple nonché gli obiettivi dell'EES, del VIS, dell'Eurodac, del SIS e [del sistema ECRIS-TCN] è istituito un servizio comune di confronto biometrico (BMS comune) che conserva i template biometrici e consente di effettuare interrogazioni con dati biometrici trasversalmente in più sistemi di informazione dell'UE.

2. Il servizio comune di confronto biometrico è composto di:

   (a) un'infrastruttura centrale, che comprende un motore di ricerca e un dispositivo per la conservazione dei dati di cui all'articolo 13;

   (b) un'infrastruttura di comunicazione sicura tra il servizio comune di confronto biometrico, il SIS centrale e l'archivio comune di dati di identità.

3. eu-LISA provvede allo sviluppo del servizio comune di confronto biometrico e ne assicura la gestione tecnica.

Articolo 13
Dati conservati nel servizio comune di confronto biometrico

1. Il servizio comune di confronto biometrico conserva i template biometrici che ottiene dai seguenti dati biometrici:

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

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

   (c) [i dati di cui all'articolo 20, paragrafo 2, lettere w) e x), del regolamento sul SIS nel settore delle verifiche di frontiera;

   (d) i dati di cui all'articolo 20, paragrafo 3, lettere w) e x), del regolamento sul SIS nel settore dell'attività di contrasto;

   (e) i dati di cui all'articolo 4, paragrafo 3, lettere t) e u), del regolamento sul SIS nel settore del rimpatrio;]

   (f) [i dati di cui all'articolo 13, lettera a), del regolamento Eurodac;]

   (g) [i dati di cui all'articolo 5, paragrafo 1, lettera b), e all'articolo 5, paragrafo 2, del regolamento ECRIS-TCN.]

2. Il servizio comune di confronto biometrico inserisce in ogni template biometrico un riferimento ai sistemi di informazione in cui sono conservati i corrispondenti dati biometrici.

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

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

Articolo 14
Ricerca di dati biometrici tramite il servizio comune di confronto biometrico

Per la ricerca dei dati biometrici conservati al loro interno, l'archivio comune di dati di identità e il SIS usano i template biometrici conservati nel servizio comune di confronto biometrico. Le interrogazioni con dati biometrici sono effettuate per le finalità del presente regolamento, del regolamento EES, del regolamento VIS, del regolamento Eurodac, [dei regolamenti SIS] e [del regolamento ECRIS-TCN].

Articolo 15
Periodo di conservazione dei dati nel servizio comune di confronto biometrico

I dati di cui all'articolo 13 sono conservati nel servizio comune di confronto biometrico per il tempo in cui i corrispondenti dati biometrici sono conservati nell'archivio comune di dati di identità o nel SIS.

Articolo 16
Registrazioni

1. Fatti salvi [l'articolo 39 del regolamento Eurodac], [gli articoli 12 e 18 del regolamento sul SIS nel settore dell'attività di contrasto] e [l'articolo 29 del regolamento ECRIS-TCN], eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nel servizio comune di confronto biometrico. Tali registrazioni comprendono, in particolare, i seguenti elementi:

   (a) lo storico della creazione e della conservazione dei template biometrici;

   (b) un riferimento ai sistemi di informazione dell'UE interrogati con i template biometrici conservati nel servizio comune di confronto biometrico;

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

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

   (e) la durata dell'interrogazione;

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

   (g) conformemente alle disposizioni nazionali, al regolamento (UE) 2016/794 o, se applicabile, al regolamento (CE) 45/2001, l'identificazione della persona che ha effettuato l'interrogazione.

2. Le registrazioni possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza degli stessi ai sensi

dell'articolo 42. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione, a meno che non siano necessarie per procedure di monitoraggio già avviate. Le registrazioni di cui al paragrafo 1, lettera a), sono cancellate non appena sono cancellati i dati.

CAPO IV
Archivio comune di dati di identità

Articolo 17
Archivio comune di dati di identità

1. Al fine di agevolare e contribuire alla corretta identificazione delle persone registrate nell'EES, nel VIS, [nell'ETIAS], nell'Eurodac e [nel sistema ECRIS-TCN], sostenere il funzionamento del rilevatore di identità multiple e agevolare e semplificare alle autorità di contrasto l'accesso ai sistemi di informazione estranei al settore del contrasto a livello dell'UE quando necessario a fini di prevenzione, indagine, accertamento o perseguimento di reati gravi, è istituito un archivio comune di dati di identità (CIR) che, per ciascuna persona registrata nell'EES, nel VIS, [nell'ETIAS], nell'Eurodac o [nel sistema ECRIS-TCN], crea un fascicolo individuale contenente i dati di cui all'articolo 18.

2. L'archivio comune di dati di identità è composto di:

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

   (b) un canale di comunicazione sicuro tra l'archivio comune di dati di identità, gli Stati membri e gli organi dell'UE autorizzati ad usare il portale di ricerca europeo conformemente al diritto dell'Unione;

   (c) un'infrastruttura di comunicazione sicura tra l'archivio comune di dati di identità e l'EES, il VIS, [l'ETIAS], l'Eurodac e [il sistema ECRIS-TCN] nonché tra l'archivio comune e le infrastrutture centrali del portale di ricerca europeo, del servizio comune di confronto biometrico e del rilevatore di identità multiple.

3. eu-LISA provvede allo sviluppo dell'archivio comune di dati di identità e ne assicura la gestione tecnica.

Articolo 18
Dati dell'archivio comune di dati di identità

1. L'archivio comune di dati di identità conserva i seguenti dati, separati per logica in base al sistema di informazione di provenienza:

   (a) – (non pertinente);

   (b) – (non pertinente);

   (c) – (non pertinente);

   (d) [i dati di cui all'articolo 13, lettere da a) a e), g) e h), del regolamento Eurodac;]

(e) [i dati di cui all'articolo 5, paragrafo 1, lettera b), e all'articolo 5, paragrafo 2, del regolamento ECRIS-TCN e i seguenti dati di cui all'articolo 5, paragrafo 1, lettera a), del medesimo regolamento: cognome; nome o nomi; sesso; data di nascita; luogo e paese di nascita; la o le cittadinanze; sesso e, se del caso, nomi precedenti e pseudonimi.

2. Per ciascuna serie di dati di cui al paragrafo 1 l'archivio comune di dati di identità inserisce un riferimento ai sistemi di informazione cui appartengono i dati.

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

Articolo 19

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

1. Qualora nell'Eurodac o [nel sistema ECRIS-TCN] siano aggiunti, modificati o cancellati dati, sono aggiunti, modificati o cancellati di conseguenza, in modo automatizzato, i dati di cui all'articolo 18 conservati nel fascicolo individuale dell'archivio comune di dati di identità.

2. Qualora il rilevatore di identità multiple crei un collegamento bianco o rosso, conformemente all'articolo 32 o all'articolo 33, tra i dati di due o più sistemi di informazione dell'UE che compongono l'archivio comune di dati di identità, quest'ultimo non crea un nuovo fascicolo individuale, bensì aggiunge i nuovi dati al fascicolo individuale dei dati oggetto del collegamento.

Articolo 20

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

1. L'autorità di polizia di uno Stato membro appositamente autorizzata da una misura legislativa nazionale di cui al paragrafo 2 può, unicamente ai fini dell'identificazione di una persona, interrogare l'archivio comune di dati di identità con i dati biometrici dell'interessato acquisiti durante una verifica d'identità.

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

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

2. Gli Stati membri che intendono valersi della possibilità offerta dal presente articolo adottano misure legislative nazionali. Tali misure specificano le finalità esatte delle verifiche di identità nell'ambito degli obiettivi di cui all'articolo 2, paragrafo 1, lettere b) e c). Designano le autorità di polizia competenti e stabiliscono le procedure, le condizioni e i criteri di tali verifiche.

Articolo 21

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

1. Se un'interrogazione dell'archivio comune di dati di identità dà luogo a un collegamento giallo conformemente all'articolo 28, paragrafo 4, l'autorità responsabile della verifica delle identità diverse determinata conformemente

all'articolo 29 ha accesso, unicamente ai fini della verifica, ai dati di identità conservati nell'archivio comune appartenenti ai vari sistemi di informazione interessati dal collegamento giallo.

2. Se un'interrogazione dell'archivio comune di dati di identità dà luogo a un collegamento rosso conformemente all'articolo 32, le autorità di cui all'articolo 26, paragrafo 2, hanno accesso, unicamente a fini di contrasto della frode di identità, ai dati di identità conservati nell'archivio comune appartenenti ai vari sistemi di informazione interessati dal collegamento rosso.

Articolo 22
Interrogazione dell'archivio comune di dati di identità a fini di contrasto

1. Le autorità designate degli Stati membri e Europol possono consultare l'archivio comune di dati di identità per prevenire, accertare o indagare reati di terrorismo o altri reati gravi in un caso specifico e per sapere se nell'Eurodac sono presenti dati su una determinata persona.

2. Quando consultano l'archivio comune ai fini di cui al paragrafo 1, le autorità designate degli Stati membri e Europol non sono autorizzati a consultare i dati appartenenti al [sistema ECRIS-TCN].

3. Se nell'Eurodac sono presenti dati sulla persona in questione, l'archivio comune risponde all'interrogazione fornendo alle autorità designate degli Stati membri e a Europol un riferimento al sistema di informazione che contiene i corrispondenti dati di cui all'articolo 18, paragrafo 2. L'archivio comune risponde con modalità che non compromettano la sicurezza dei dati.

4. Il pieno accesso ai dati contenuti nei sistemi di informazione dell'UE a fini di prevenzione, accertamento e indagine di reati di terrorismo o altri reati gravi è soggetto alle condizioni e procedure previste nei rispettivi strumenti legislativi che disciplinano tale accesso.

Articolo 23
Periodo di conservazione dei dati nell'archivio comune di dati di identità

1. I dati di cui all'articolo 18, paragrafi 1 e 2, sono cancellati dall'archivio comune di dati di identità conformemente alle disposizioni in materia di conservazione dei dati [del regolamento Eurodac] e [del regolamento ECRIS-TCN] rispettivamente.

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

Articolo 24
Registrazioni

1. Fatti salvi [l'articolo 39 del regolamento Eurodac] e [l'articolo 29 del regolamento ECRIS-TCN], eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nell'archivio comune di dati di identità conformemente ai paragrafi 2, 3 e 4.

2. Per qualsiasi accesso all'archivio comune di dati di identità ai sensi dell'articolo 20, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nell'archivio comune. Tali registrazioni comprendono, in particolare, i seguenti elementi:

   (a) la finalità dell'accesso dell'utente che effettua l'interrogazione tramite l'archivio comune;

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

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

   (d) i risultati dell'interrogazione;

   (e) conformemente alle disposizioni nazionali, al regolamento (UE) 2016/794 o, se applicabile, al regolamento (CE) 45/2001, l'identificazione della persona che ha effettuato l'interrogazione.

3. Per qualsiasi accesso all'archivio comune di dati di identità ai sensi dell'articolo 21, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nell'archivio comune. Tali registrazioni comprendono, in particolare, i seguenti elementi:

   (a) la finalità dell'accesso dell'utente che effettua l'interrogazione tramite l'archivio comune;

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

   (c) se del caso, i dati usati per avviare l'interrogazione;

   (d) se del caso, i risultati dell'interrogazione;

   (e) conformemente alle disposizioni nazionali, al regolamento (UE) 2016/794 o, se applicabile, al regolamento (CE) 45/2001, l'identificazione della persona che ha effettuato l'interrogazione.

4. Per qualsiasi accesso all'archivio comune di dati di identità ai sensi dell'articolo 22, eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati effettuate nell'archivio comune. Tali registrazioni comprendono, in particolare, i seguenti elementi:

   (a) il riferimento del fascicolo nazionale;

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

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

   (d) i risultati dell'interrogazione;

   (e) il nome dell'autorità che consulta l'archivio comune;

   (f) conformemente alle disposizioni nazionali, al regolamento (UE) 2016/794 o, se applicabile, al regolamento (CE) 45/2001, l'identificazione del funzionario che ha effettuato l'interrogazione e del funzionario che ha ordinato l'interrogazione.

   Le autorità di controllo competenti istituite conformemente all'articolo 51 del regolamento (UE) 2016/679 o all'articolo 41 della direttiva 2016/680 verificano periodicamente, a intervalli non superiori a sei mesi, le registrazioni dell'accesso per controllare il rispetto delle procedure e delle condizioni di cui all'articolo 22, paragrafi da 1 a 3.

5. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dal personale debitamente autorizzato a usare l'archivio comune di dati di identità ai sensi degli articoli 20, 21 e 22.

6. Le registrazioni di cui ai paragrafi 1 e 5 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità della richiesta e della liceità del trattamento dei dati, e per garantire la sicurezza degli stessi ai sensi dell'articolo 42. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione, a meno che non siano necessarie per procedure di monitoraggio già avviate.

7. Ai fini ai cui al paragrafo 6, eu-LISA conserva le registrazioni relative allo storico dei dati conservati nel fascicolo individuale. Le registrazioni relative allo storico dei dati conservati sono cancellate non appena sono cancellati i dati.

CAPO V
Rilevatore di identità multiple

Articolo 25
Rilevatore di identità multiple

1. Al fine di sostenere il funzionamento dell'archivio comune di dati di identità e gli obiettivi dell'EES, del VIS, [dell'ETIAS], dell'Eurodac, del SIS e [del sistema ECRIS-TCN] è istituito un rilevatore di identità multiple (MID) che crea e conserva collegamenti tra dati dei sistemi di informazione dell'UE inclusi nell'archivio comune e dati del SIS e che, di conseguenza, rileva le identità multiple, al duplice scopo di agevolare le verifiche di identità e contrastare la frode di identità.

2. Il rilevatore di identità multiple è composto di:

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

   (b) un'infrastruttura di comunicazione sicura che collega il rilevatore di identità multiple al SIS e alle infrastrutture centrali del portale di ricerca europeo e dell'archivio comune di dati di identità.

3. eu-LISA provvede allo sviluppo del rilevatore di identità multiple e ne assicura la gestione tecnica.

Articolo 26
Accesso al rilevatore di identità multiple

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

   (a) – (non pertinente);

   (b) – (non pertinente);

   (c) – (non pertinente);

   (d) alle autorità competenti per l'esame di una domanda di protezione internazionale previste dal regolamento Eurodac quando esaminano una nuova domanda di protezione internazionale;

(e) agli uffici SIRENE degli Stati membri che creano [una segnalazione SIS conformemente al regolamento sul SIS nel settore dell'attività di contrasto e al regolamento sul SIS nel settore del rimpatrio];

(f) [all'autorità centrale dello Stato membro di condanna quando registra o aggiorna dati nel sistema ECRIS-TCN conformemente all'articolo 5 del regolamento ECRIS-TCN.]

2. Le autorità degli Stati membri e gli organi dell'UE che hanno accesso ad almeno uno dei sistemi di informazione dell'UE inclusi nell'archivio comune di dati di identità o al SIS hanno accesso ai dati di cui all'articolo 34, lettere a) e b), riguardanti i collegamenti rossi di cui all'articolo 32.

Articolo 27
Rilevazione di identità multiple

1. È avviata una procedura di rilevazione di identità multiple nell'archivio comune di dati di identità e nel SIS quando:

(a) – (non pertinente);

(b) – (non pertinente);

(c) – (non pertinente);

(d) [è creata o aggiornata una domanda di protezione internazionale nell'Eurodac conformemente all'articolo 10 del regolamento Eurodac;]

(e) [è creata o aggiornata una segnalazione su una persona nel SIS conformemente ai capi VI, VII, VIII e IX del regolamento sul SIS nel settore dell'attività di contrasto e all'articolo 3 del regolamento sul SIS nel settore del rimpatrio;]

(f) [è creato o aggiornato un record di dati nel sistema ECRIS-TCN conformemente all'articolo 5 del regolamento ECRIS-TCN.]

2. Se tra i dati di un sistema di informazione di cui al paragrafo 1 figurano dati biometrici, l'archivio comune di dati di identità e il SIS centrale effettuano la procedura di rilevazione delle identità multiple tramite il servizio comune di confronto biometrico. Il servizio comune di confronto biometrico raffronta i template biometrici ricavati dai nuovi dati biometrici con i template biometrici già presenti al suo interno e verifica se nell'archivio comune di dati di identità o nel SIS centrale sono già conservati dati dello stesso cittadino di paese terzo.

3. Oltre alla procedura di cui al paragrafo 2, l'archivio comune di dati di identità e il SIS centrale effettuano la ricerca nei dati conservati al loro interno mediante il portale di ricerca europeo usando i seguenti dati:

(a) – (non pertinente);

(b) – (non pertinente);

(c) – (non pertinente);

(d) [cognomi; nomi; nomi e cognomi alla nascita, eventuali nomi e cognomi precedenti e "alias"; data di nascita, luogo di nascita, cittadinanza o cittadinanze e sesso, conformemente all'articolo 12 del regolamento Eurodac;]

(e) – (non pertinente);

(f) [cognome/cognomi; nome/nomi; nomi e cognomi alla nascita, eventuali nomi e cognomi precedenti e "alias"; data di nascita, luogo di nascita, cittadinanza o

cittadinanze e sesso, conformemente all'articolo 20, paragrafo 3, del regolamento sul SIS nel settore dell'attività di contrasto;]

(g) [cognome/cognomi; nome/nomi; nomi e cognomi alla nascita, eventuali nomi e cognomi precedenti e "alias"; data di nascita, luogo di nascita, cittadinanza o cittadinanze e sesso, conformemente all'articolo 4 del regolamento sul SIS nel settore del rimpatrio;]

(h) [cognome; nome o nomi; data di nascita, luogo di nascita, cittadinanza o cittadinanze e sesso, conformemente all'articolo 5, paragrafo 1, lettera a), del regolamento ECRIS-TCN.]

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

Articolo 28
Esito della procedura di rilevazione di identità multiple

1. Qualora dall'interrogazione di cui all'articolo 27, paragrafo 2 o 3, non risulti alcun riscontro positivo, la pertinente procedura di cui all'articolo 27, paragrafo 1, prosegue conformemente al regolamento che la disciplina.

2. Qualora dall'interrogazione di cui all'articolo 27, paragrafo 2 o 3, risultino uno o più riscontri positivi, l'archivio comune di dati di identità e, se del caso, il SIS creano un collegamento tra i dati usati per avviare l'interrogazione e i dati per i quali è emerso il riscontro positivo.

Qualora risultino più riscontri positivi è creato un collegamento tra tutti i dati per i quali è emerso un riscontro positivo. Se i dati sono già oggetto di un collegamento, questo è esteso ai dati usati per avviare l'interrogazione.

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

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

5. La Commissione stabilisce con atti di esecuzione le procedure per determinare i casi in cui i dati di identità possono essere considerati identici o simili. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 64, paragrafo 2.

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

La Commissione stabilisce con atti di esecuzione le norme tecniche per creare i collegamenti tra i dati di diversi sistemi di informazione. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 64, paragrafo 2.

Articolo 29
Verifica manuale delle identità diverse

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

   (a) – (non pertinente);

   (b) – (non pertinente);

   (c) – (non pertinente);

   (d) l'autorità che esamina la domanda di protezione internazionale conformemente al regolamento Eurodac, per i riscontri positivi emersi durante l'esame di detta domanda;

   (e) gli uffici SIRENE degli Stati membri, per i riscontri positivi emersi durante la creazione di una segnalazione SIS conformemente [al regolamento sul SIS nel settore dell'attività di contrasto e al regolamento sul SIS nel settore del rimpatrio];

   (f) l'autorità centrale dello Stato membro di condanna, per i riscontri positivi emersi durante la registrazione o l'aggiornamento dei dati nel sistema ECRIS-TCN conformemente all'articolo 5 [del regolamento ECRIS-TCN].

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

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

   (a) in una segnalazione di persone ricercate per l'arresto a fini di consegna o di estradizione di cui all'articolo 26 [del regolamento sul SIS nel settore dell'attività di contrasto];

   (b) in una segnalazione di persone scomparse o vulnerabili di cui all'articolo 32 [del regolamento sul SIS nel settore dell'attività di contrasto];

   (c) in una segnalazione di persone ricercate per presenziare ad un procedimento giudiziario di cui all'articolo 34 [del regolamento sul SIS nel settore dell'attività di contrasto];

   (d) [in una segnalazione riguardante il rimpatrio di cui al regolamento sul SIS nel settore del rimpatrio;]

   (e) in una segnalazione di persone ai fini di controlli discreti, controlli di indagine o controlli specifici di cui all'articolo 36 [del regolamento sul SIS nel settore dell'attività di contrasto];

   (f) in una segnalazione di ignoti ricercati a fini di identificazione in conformità della legislazione nazionale e di interrogazione con dati biometrici di cui all'articolo 40 [del regolamento sul SIS nel settore dell'attività di contrasto].

3. Fatto salvo il paragrafo 4, l'autorità responsabile della verifica delle identità diverse ha accesso ai corrispondenti dati contenuti nel pertinente fascicolo di conferma dell'identità e ai dati di identità oggetto del collegamento nell'archivio comune di dati di identità e, se del caso, nel SIS, ed esamina le identità diverse, aggiorna il collegamento conformemente agli articoli 31, 32 e 33 e lo aggiunge senza indugio al fascicolo di conferma dell'identità.

4. – (non pertinente).

5. Se emerge più di un collegamento l'autorità responsabile della verifica delle identità diverse esamina ogni collegamento separatamente.

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

Articolo 30
Collegamento giallo

1. Il collegamento tra dati di due o più sistemi di informazione è classificato giallo nei seguenti casi:

   (a) il collegamento evidenzia gli stessi dati biometrici ma dati di identità differenti e non è stata svolta alcuna verifica manuale dell'identità diversa;

   (b) il collegamento evidenzia dati di identità differenti e non è stata svolta alcuna verifica manuale dell'identità diversa.

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

Articolo 31
Collegamento verde

1. Il collegamento tra dati di due o più sistemi di informazione è classificato verde quando evidenzia dati biometrici differenti ma dati di identità simili e l'autorità responsabile della verifica delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a due persone diverse.

2. Quando è interrogato l'archivio comune di dati di identità o il SIS e sussiste un collegamento verde tra due o più sistemi di informazione che costituiscono l'archivio comune o con il SIS, il rilevatore di identità multiple indica che i dati di identità oggetto del collegamento non si riferiscono alla stessa persona. Il sistema di informazione interrogato risponde indicando solo i dati della persona i cui dati sono stati usati per l'interrogazione, senza far emergere un riscontro positivo con i dati oggetto del collegamento verde.

Articolo 32
Collegamento rosso

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

   (a) il collegamento evidenzia gli stessi dati biometrici ma dati di identità differenti e l'autorità responsabile della verifica delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono alla stessa persona che usa illecitamente le identità in questione;

   (b) il collegamento evidenzia dati di identità simili e l'autorità responsabile della verifica delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono alla stessa persona che usa illecitamente le identità in questione.

2. Quando è interrogato l'archivio comune di dati di identità o il SIS e sussiste un collegamento rosso tra due o più sistemi di informazione che costituiscono l'archivio comune o con il SIS, il rilevatore di identità multiple risponde indicando i dati di cui all'articolo 34. Al collegamento rosso è dato seguito conformemente al diritto dell'Unione e nazionale.

3. Qualora sia creato un collegamento rosso tra dati dell'EES, del VIS, [dell'ETIAS], dell'Eurodac o [del sistema ECRIS-TCN], il fascicolo individuale conservato nell'archivio comune di dati di identità è aggiornato conformemente all'articolo 19, paragrafo 1.

4. Fatte salve le disposizioni relative al trattamento delle segnalazioni nel SIS di cui [al regolamento sul SIS nel settore delle verifiche di frontiera, al regolamento sul SIS nel settore dell'attività di contrasto e al regolamento sul SIS nel settore del rimpatrio] e le limitazioni necessarie per proteggere la sicurezza e l'ordine pubblico, prevenire la criminalità e garantire che non siano compromesse indagini nazionali, qualora sia creato un collegamento rosso l'autorità responsabile della verifica delle identità diverse informa la persona interessata della presenza di identità multiple illecite.

5. Qualora sia creato un collegamento rosso l'autorità responsabile della verifica delle identità diverse mette un riferimento alle autorità responsabili dei dati oggetto del collegamento.

Articolo 33
Collegamento bianco

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

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

   (b) il collegamento evidenzia dati di identità identici o simili e almeno uno dei sistemi di informazione non contiene dati biometrici della persona in questione;

   (c) il collegamento evidenzia gli stessi dati biometrici ma dati di identità differenti e l'autorità responsabile della verifica delle identità diverse ha concluso che i dati oggetto del collegamento si riferiscono a una stessa persona che lecitamente possiede dati di identità diversi.

2. Quando è interrogato l'archivio comune di dati di identità o il SIS e sussiste un collegamento bianco tra uno o più sistemi di informazione che costituiscono l'archivio comune o con il SIS, il rilevatore di identità multiple indica che i dati di identità oggetto del collegamento si riferiscono alla stessa persona. Se l'autorità che ha avviato l'interrogazione ha accesso ai dati oggetto del collegamento in base al diritto dell'Unione o nazionale, i sistemi di informazione interrogati rispondono indicando, se del caso, tutti i dati oggetto del collegamento riguardanti la persona, facendo così emergere un riscontro positivo con i dati oggetto del collegamento bianco.

3. Qualora sia creato un collegamento bianco tra dati dell'EES, del VIS, [dell'ETIAS], dell'Eurodac o [del sistema ECRIS-TCN], il fascicolo individuale conservato nell'archivio comune di dati di identità è aggiornato conformemente all'articolo 19, paragrafo 1.

4. Fatte salve le disposizioni relative al trattamento delle segnalazioni nel SIS di cui [al regolamento sul SIS nel settore delle verifiche di frontiera, al regolamento sul SIS

nel settore dell'attività di contrasto e al regolamento sul SIS nel settore del rimpatrio], qualora sia creato un collegamento bianco a seguito di una verifica manuale delle identità diverse, l'autorità responsabile della verifica delle identità diverse informa la persona interessata della presenza di discrepanze tra i diversi sistemi quanto ai dati personali che la riguardano e mette un riferimento alle autorità responsabili dei dati oggetto del collegamento.

Articolo 34
Fascicolo di conferma dell'identità

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

(a) i collegamenti, con indicazione del colore conformemente agli articoli da 30 a 33;

(b) un riferimento ai sistemi di informazione i cui dati sono oggetto del collegamento;

(c) un numero di identificazione unico che permette di estrarre i dati dai sistemi di informazione cui appartengono i fascicoli corrispondenti oggetto del collegamento;

(d) se del caso, l'autorità responsabile della verifica delle identità diverse.

Articolo 35
Conservazione dei dati nel rilevatore di identità multiple

I fascicoli di conferma dell'identità e i relativi dati, compresi i collegamenti, sono conservati nel rilevatore di identità multiple solo per il tempo in cui i dati oggetto del collegamento sono conservati in due o più sistemi di informazione dell'UE.

Articolo 36
Registrazioni

1. eu-LISA conserva le registrazioni di tutti i trattamenti di dati nel rilevatore di identità multiple. Tali registrazioni comprendono, in particolare, i seguenti elementi:

   (a) la finalità dell'accesso dell'utente e i suoi diritti di accesso;

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

   (c) il tipo di dati usati per avviare la o le interrogazioni;

   (d) il riferimento ai dati oggetto del collegamento;

   (e) lo storico del fascicolo di conferma dell'identità;

   (f) l'identificazione della persona che ha effettuato l'interrogazione.

2. Ciascuno Stato membro conserva le registrazioni del personale debitamente autorizzato a usare il rilevatore di identità multiple.

3. Le registrazioni possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità della richiesta e della liceità del trattamento dei dati, e per garantire la sicurezza degli stessi ai sensi dell'articolo 42. Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione, a meno che non

siano necessarie per procedure di monitoraggio già avviate. Le registrazioni relative allo storico del fascicolo di conferma dell'identità sono cancellate non appena sono cancellati i dati del fascicolo di conferma dell'identità.

CAPO VI
Misure a sostegno dell'interoperabilità

Articolo 37
Qualità dei dati

1. eu-LISA istituisce procedure e meccanismi automatizzati di controllo della qualità dei dati per i dati conservati nel SIS, nell'Eurodac, [nel sistema ECRIS-TCN], nel servizio comune di confronto biometrico, nell'archivio comune di dati di identità e nel rilevatore di identità multiple.

2. eu-LISA istituisce indicatori comuni della qualità dei dati e norme minime di qualità per conservare i dati nel SIS, nell'Eurodac, [nel sistema ECRIS-TCN], nel servizio comune di confronto biometrico, nell'archivio comune di dati di identità e nel rilevatore di identità multiple.

3. eu-LISA riferisce periodicamente agli Stati membri in merito alle procedure e ai meccanismi automatizzati di controllo della qualità dei dati e agli indicatori comuni della qualità dei dati. eu-LISA riferisce periodicamente alla Commissione in merito ai problemi incontrati e agli Stati membri interessati.

4. I dettagli delle procedure e dei meccanismi automatizzati di controllo della qualità dei dati, gli indicatori comuni della qualità dei dati e le norme minime di qualità per conservare i dati nel SIS, nell'Eurodac, [nel sistema ECRIS-TCN], nel SIS, nel servizio comune di confronto biometrico, nell'archivio comune di dati di identità e nel rilevatore di identità multiple, segnatamente per quanto riguarda i dati biometrici, sono stabiliti con atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 64, paragrafo 2.

5. Un anno dopo l'istituzione delle procedure e dei meccanismi automatizzati di controllo della qualità dei dati e degli indicatori comuni della qualità dei dati, e successivamente ogni anno, la Commissione valuta l'attuazione da parte degli Stati membri dei requisiti di qualità dei dati e formula le eventuali raccomandazioni necessarie. Gli Stati membri presentano alla Commissione un piano d'azione volto a correggere le carenze riscontrate nella relazione di valutazione e riferiscono sui progressi compiuti con il piano d'azione fino alla sua completa attuazione. La Commissione trasmette la relazione di valutazione al Parlamento europeo, al Consiglio, al garante europeo della protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali istituita con regolamento (CE) n. 168/2007 del Consiglio[63].

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

Articolo 38
Formato universale dei messaggi

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

2. Lo standard UMF è usato per lo sviluppo dell'[Eurodac], [del sistema ECRIS-TCN], del portale di ricerca europeo, dell'archivio comune di dati di identità, del rilevatore di identità multiple e, se del caso, per lo sviluppo da parte di eu-LISA o di altro organo dell'UE di nuovi modelli per lo scambio di informazioni o nuovi sistemi di informazione del settore Giustizia e affari interni.

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

4. Ai fini dell'istituzione e dello sviluppo dello standard UMF la Commissione adotta atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 64, paragrafo 2.

Articolo 39
Archivio centrale di relazioni e statistiche

1. È istituito un archivio centrale di relazioni e statistiche (CRRS) al fine di sostenere gli obiettivi dell'Eurodac, del SIS e [del sistema ECRIS-TCN] e generare dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati.

2. eu-LISA istituisce, attua e ospita l'archivio centrale di relazioni e statistiche nei suoi siti tecnici contenenti, separati per logica, i dati di cui [all'articolo 42, paragrafo 8, del regolamento Eurodac], [all'articolo 71 del regolamento sul SIS nel settore dell'attività di contrasto] e [all'articolo 30 del regolamento sul sistema ECRIS-TCN]. I dati contenuti nell'archivio centrale di relazioni e statistiche non consentono l'identificazione delle persone fisiche. L'accesso all'archivio è concesso mediante un accesso sicuro tramite la rete di servizi transeuropei sicuri per la comunicazione telematica tra amministrazioni (TESTA) con controllo dell'accesso e specifici profili di utente, unicamente ai fini dell'elaborazione di relazioni e statistiche, alle autorità di cui [all'articolo 42, paragrafo 8, del regolamento Eurodac], [all'articolo 71 del regolamento sul SIS nel settore dell'attività di contrasto] e [all'articolo 30 del regolamento sul sistema ECRIS-TCN].

3. eu-LISA anonimizza i dati e li registra nell'archivio centrale di relazioni e statistiche. Il processo di anonimizzazione dei dati è automatizzato.

4. L'archivio centrale di relazioni e statistiche è composto di:

   (a) un'infrastruttura centrale, costituita da un archivio di dati che consente l'anonimizzazione;

   (b) un'infrastruttura di comunicazione sicura per collegare l'archivio centrale di relazioni e statistiche al SIS, all'Eurodac e [al sistema ECRIS-TCN], nonché alle infrastrutture centrali del servizio comune di confronto biometrico, dell'archivio comune di dati di identità e del rilevatore di identità multiple.

5. La Commissione stabilisce con atti di esecuzione le modalità di funzionamento dell'archivio centrale di relazioni e statistiche, comprese le garanzie specifiche per il trattamento dei dati personali di cui ai paragrafi 2 e 3 e le norme di sicurezza applicabili all'archivio. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 64, paragrafo 2.

CAPO VII
Protezione dei dati

Articolo 40
Titolare del trattamento

1. Per quanto riguarda il trattamento dei dati nel servizio comune di confronto biometrico, le autorità degli Stati membri titolari del trattamento per l'Eurodac, il SIS e [il sistema ECRIS-TCN], rispettivamente, sono considerate titolari del trattamento ai sensi dell'articolo 4, punto 7, del regolamento (UE) 2016/679 in relazione ai template biometrici ottenuti dai dati di cui all'articolo 13 inseriti da ciascuna autorità nel rispettivo sistema e hanno la responsabilità del trattamento dei template biometrici nel servizio comune di confronto biometrico.

2. Per quanto riguarda il trattamento dei dati nell'archivio comune di dati di identità, le autorità degli Stati membri titolari del trattamento per l'Eurodac e [il sistema ECRIS-TCN], rispettivamente, sono considerate titolari del trattamento ai sensi dell'articolo 4, punto 7, del regolamento (UE) 2016/679 in relazione ai dati di cui all'articolo 18 inseriti da ciascuna autorità nel rispettivo sistema e hanno la responsabilità del trattamento di tali dati personali nell'archivio comune.

3. Per quanto riguarda il trattamento dei dati nel rilevatore di identità multiple:

   (a) l'Agenzia europea della guardia di frontiera e costiera è considerata responsabile del trattamento ai sensi dell'articolo 2, lettera b), del regolamento (CE) n. 45/2001 in relazione al trattamento di dati personali da parte dell'unità centrale ETIAS;

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

Articolo 41
Responsabile del trattamento

Per quanto riguarda il trattamento dei dati personali nell'archivio comune di dati di identità, eu-LISA è considerata incaricato del trattamento ai sensi dell'articolo 2, lettera e), del regolamento (CE) n. 45/2001.

Articolo 42
Sicurezza del trattamento

1. eu-LISA e le autorità degli Stati membri garantiscono la sicurezza del trattamento di dati personali svolto in applicazione del presente regolamento. eu-LISA, [l'unità

centrale ETIAS] e le autorità degli Stati membri cooperano nei compiti relativi alla sicurezza.

2. Fatto salvo l'articolo 22 del regolamento (CE) n. 45/2001, eu-LISA adotta le misure necessarie per garantire la sicurezza delle componenti dell'interoperabilità e delle relative infrastrutture di comunicazione.

3. In particolare eu-LISA adotta le misure necessarie, compresi un piano di sicurezza, un piano di continuità operativa e un piano di ripristino in caso di disastro, al fine di:

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

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

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

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

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

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

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

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

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

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

Articolo 43
Riservatezza dei dati SIS

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

2. Fatto salvo l'articolo 17 dello statuto dei funzionari dell'Unione europea e regime applicabile agli altri agenti dell'Unione europea, eu-LISA applica norme adeguate in materia di segreto professionale o altri obblighi di riservatezza equivalenti a tutti i membri del proprio personale che debbano lavorare con i dati SIS, secondo standard equiparabili a quelli previsti al paragrafo 1. Tale obbligo vincola gli interessati anche dopo che hanno lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

Articolo 44
Incidenti di sicurezza

1. È considerato incidente di sicurezza l'evento che ha o può avere ripercussioni sulla sicurezza delle componenti dell'interoperabilità e può causare danni o perdite ai dati ivi conservati, in particolare quando possono essere stati consultati dati senza autorizzazione o quando sono state o possono essere state compromesse la disponibilità, l'integrità e la riservatezza dei dati.
2. Ogni incidente di sicurezza è gestito in modo da garantire una risposta rapida, efficace e adeguata.
3. Fatte salve la notifica e la comunicazione di una violazione dei dati personali a norma dell'articolo 33 del regolamento (UE) 2016/679, dell'articolo 30 della direttiva (UE) 2016/680, o di entrambi, gli Stati membri notificano gli incidenti di sicurezza alla Commissione, a eu-LISA e al garante europeo della protezione dei dati. Qualora si verifichi un incidente di sicurezza in relazione all'infrastruttura centrale delle componenti dell'interoperabilità, eu-LISA ne dà notifica alla Commissione e al garante europeo della protezione dei dati.
4. Le informazioni sull'incidente di sicurezza che ha o può avere ripercussioni sul funzionamento delle componenti dell'interoperabilità o sulla disponibilità, integrità e riservatezza dei dati sono fornite agli Stati membri e registrate secondo il piano di gestione degli incidenti stabilito da eu-LISA.
5. Gli Stati membri interessati e eu-LISA cooperano in caso di incidente di sicurezza. La Commissione stabilisce con atti di esecuzione le modalità di tale procedura di cooperazione. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 64, paragrafo 2.

Articolo 45
Verifica interna

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

I titolari del trattamento di cui all'articolo 40 prendono le misure necessarie per verificare la conformità del trattamento dei dati a norma del presente regolamento, tra cui la verifica frequente delle registrazioni, e cooperare, laddove necessario, con le autorità di controllo di cui agli articoli 49 e 50.

Articolo 46
Diritto di informazione

1. Fatto salvo il diritto di informazione di cui agli articoli 11 e 12 del regolamento (CE) n. 45/2001 e agli articoli 13 e 14 del regolamento (UE) 2016/679, le persone i cui dati sono conservati nel servizio comune di confronto biometrico, nell'archivio comune di dati di identità o nel rilevatore di identità multiple sono informate dall'autorità che raccoglie i dati che le riguardano, al momento della raccolta, in merito al trattamento dei dati personali ai fini del presente regolamento, all'identità e ai dati di contatto del rispettivo titolare del trattamento e alle procedure per esercitare i diritti di accesso, rettifica e cancellazione nonché in merito ai dati di contatto del garante europeo della protezione dei dati e dell'autorità nazionale di controllo dello Stato membro responsabile della raccolta dei dati.

2. Le persone i cui dati sono registrati nell'Eurodac o [nel sistema ECRIS-TCN] sono informate del trattamento dei dati ai fini del presente regolamento conformemente al paragrafo 1 quando:

   (a) – (non pertinente);

   (b) – (non pertinente);

   (c) – (non pertinente);

   (d) [è creata o aggiornata una domanda di protezione internazionale nell'Eurodac conformemente all'articolo 10 del regolamento Eurodac;]

   (e) [è creato o aggiornato un record di dati nel sistema ECRIS-TCN conformemente all'articolo 5 del regolamento ECRIS-TCN.]

Articolo 47
Diritto di accesso, rettifica e cancellazione

1. Per esercitare i diritti di cui agli articoli 13, 14, 15 e 16 del regolamento (CE) n. 45/2001 e agli articoli 15, 16, 17 e 18 del regolamento (UE) 2016/679, l'interessato ha il diritto di rivolgersi allo Stato membro competente della verifica manuale delle identità diverse o a qualsiasi altro Stato membro, che esamina la richiesta e vi risponde.

2. Lo Stato membro competente della verifica manuale delle identità diverse di cui all'articolo 29 o lo Stato membro al quale è stata presentata la richiesta risponde entro 45 giorni dalla ricezione della richiesta.

3. Qualora la richiesta di rettifica o cancellazione dei dati personali sia presentata a uno Stato membro diverso da quello competente, lo Stato membro al quale è stata presentata contatta le autorità dello Stato membro competente entro sette giorni e quest'ultimo verifica, entro 30 giorni da tale contatto, l'esattezza dei dati e la liceità del loro trattamento.

4. Qualora da un esame emerga che i dati conservati nel rilevatore di identità multiple sono di fatto inesatti o sono stati registrati illecitamente, lo Stato membro competente o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta provvede a rettificare o cancellare i dati.

5. Qualora i dati nel rilevatore di identità multiple siano modificati dallo Stato membro competente durante il loro periodo di validità, lo Stato membro competente effettua il trattamento di cui all'articolo 27 e, se del caso, all'articolo 29 per determinare se i

dati modificati debbano essere oggetto di un collegamento. Qualora dal trattamento non risulti alcun riscontro positivo, lo Stato membro competente o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta provvede a cancellare i dati dal fascicolo di conferma dell'identità. Qualora dal trattamento automatizzato risultino uno o più riscontri positivi, lo Stato membro competente crea o aggiorna il relativo collegamento conformemente alle disposizioni pertinenti del presente regolamento.

6. Qualora non ritenga che i dati conservati nel rilevatore di identità multiple siano di fatto inesatti o siano stati registrati illecitamente, lo Stato membro competente o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta adotta una decisione amministrativa con la quale illustra per iscritto senza indugio all'interessato la ragione per cui non intende rettificare o cancellare i dati che lo riguardano.

7. Detta decisione fornisce all'interessato informazioni sulla possibilità di impugnare la decisione adottata sulla richiesta di cui al paragrafo 3 e, se del caso, informazioni su come intentare un'azione o presentare un reclamo dinanzi alle autorità competenti o alle autorità giurisdizionali competenti e su qualunque tipo di assistenza, anche da parte delle autorità nazionali di controllo competenti.

8. La richiesta presentata a norma del paragrafo 3 contiene le informazioni necessarie per identificare l'interessato. Tali informazioni sono utilizzate unicamente per consentire l'esercizio dei diritti di cui al paragrafo 3 e sono cancellate subito dopo.

9. Lo Stato membro competente o, ove applicabile, lo Stato membro al quale è stata presentata la richiesta conserva una registrazione, sotto forma di documento scritto, della presentazione di una richiesta ai sensi del paragrafo 3 e di come è stata trattata e mette senza indugio tale documento a disposizione delle competenti autorità nazionali di controllo per la protezione dei dati.

Articolo 48

Comunicazione di dati personali a paesi terzi, organizzazioni internazionali e soggetti privati

I dati personali conservati nelle componenti dell'interoperabilità o da queste consultati non sono trasferiti a paesi terzi, organizzazioni internazionali o soggetti privati, né sono messi a loro disposizione.

Articolo 49

Controllo dell'autorità nazionale di controllo

1. L'autorità o le autorità di controllo designate in conformità dell'articolo 49 del regolamento (UE) 2016/679 provvedono affinché, almeno ogni quattro anni, sia svolto un audit dei trattamenti di dati da parte delle autorità nazionali competenti conformemente ai pertinenti principi internazionali di audit.

2. Gli Stati membri provvedono affinché la propria autorità di controllo disponga delle risorse sufficienti per assolvere i compiti ad essa affidati dal presente regolamento.

Articolo 50

Controllo del garante europeo della protezione dei dati

Il garante europeo della protezione dei dati provvede affinché almeno ogni quattro anni sia svolto un audit delle attività di trattamento dei dati personali effettuate da eu-LISA

conformemente ai pertinenti principi internazionali di audit. Una relazione su tale audit è trasmessa al Parlamento europeo, al Consiglio, a eu-LISA, alla Commissione e agli Stati membri. A eu-LISA è data la possibilità di presentare osservazioni prima dell'adozione della relazione.

Articolo 51
Cooperazione tra le autorità nazionali di controllo e il garante europeo della protezione dei dati

1. Il garante europeo della protezione dei dati agisce in stretta cooperazione con le autorità nazionali di controllo riguardo a temi specifici che richiedono un contributo nazionale, in particolare se il garante europeo della protezione dei dati o un'autorità nazionale di controllo constata notevoli differenze tra le pratiche degli Stati membri o trasferimenti potenzialmente illeciti nell'uso dei canali di comunicazione delle componenti dell'interoperabilità, o in relazione a questioni sollevate da una o più autorità nazionali di controllo sull'attuazione e interpretazione del presente regolamento.

2. Nei casi di cui al paragrafo 1 è assicurato il controllo coordinato a norma dell'articolo 62 del regolamento (UE) XXXX/2018 [revisione del regolamento 45/2001].

Capo VIII
Responsabilità

Articolo 52
Responsabilità di eu-LISA nella fase di progettazione e sviluppo

1. eu-LISA garantisce che le infrastrutture centrali delle componenti dell'interoperabilità siano gestite conformemente al presente regolamento.

2. Le componenti dell'interoperabilità sono ospitate da eu-LISA nei suoi siti tecnici e forniscono le funzionalità di cui al presente regolamento nel rispetto delle condizioni di sicurezza, disponibilità, qualità e rapidità di cui all'articolo 53, paragrafo 1.

3. eu-LISA è responsabile dello sviluppo delle componenti dell'interoperabilità e di ogni adattamento necessario per istituire l'interoperabilità tra i sistemi centrali dell'EES, del VIS, [dell'ETIAS], del SIS, dell'Eurodac e [del sistema ECRIS-TCN] e il portale di ricerca europeo, il servizio comune di confronto biometrico, l'archivio comune di dati di identità e il rilevatore di identità multiple.

   eu-LISA definisce la progettazione dell'architettura fisica delle componenti dell'interoperabilità, comprese le rispettive infrastrutture di comunicazione, e le specifiche tecniche e la loro evoluzione per quanto riguarda l'infrastruttura centrale e l'infrastruttura di comunicazione sicura, che sono adottate dal consiglio di amministrazione previo parere favorevole della Commissione. eu-LISA provvede anche agli adattamenti del SIS, dell'Eurodac o [del sistema ECRIS-TCN] resi necessari dall'interoperabilità e previsti dal presente regolamento.

   eu-LISA sviluppa e implementa le componenti dell'interoperabilità non appena possibile dopo l'entrata in vigore del presente regolamento e l'adozione da parte della Commissione delle misure di cui all'articolo 8, paragrafo 2, all'articolo 9,

paragrafo 7, all'articolo 28, paragrafi 5 e 6, all'articolo 37, paragrafo 4, all'articolo 38, paragrafo 4, all'articolo 39, paragrafo 5, e all'articolo 44, paragrafo 5.

Lo sviluppo comporta l'elaborazione e l'applicazione delle specifiche tecniche, il collaudo e il coordinamento generale del progetto.

4. In fase di progettazione e di sviluppo, è istituito un consiglio di gestione del programma composto di un massimo di 10 membri. Esso è costituito da sette membri nominati dal consiglio di amministrazione di eu-LISA tra i suoi membri o i supplenti, dal presidente del gruppo consultivo sull'interoperabilità di cui all'articolo 65, da un membro che rappresenta eu-LISA nominato dal suo direttore esecutivo e da un membro nominato dalla Commissione. I membri nominati dal consiglio di amministrazione di eu-LISA sono eletti soltanto tra gli Stati membri che sono pienamente vincolati, in base al diritto dell'Unione, dagli strumenti legislativi che disciplinano lo sviluppo, l'istituzione, il funzionamento e l'uso di tutti i sistemi IT su larga scala gestiti da eu-LISA e che partecipano alle componenti dell'interoperabilità.

5. Il consiglio di gestione del programma si riunisce periodicamente, almeno tre volte a trimestre. Esso garantisce l'adeguata gestione della fase di progettazione e sviluppo delle componenti dell'interoperabilità.

Il consiglio di gestione del programma presenta mensilmente relazioni scritte al consiglio di amministrazione sui progressi del progetto. Il consiglio di gestione del programma non ha potere decisionale, né mandato di rappresentare i membri del consiglio di amministrazione di eu-LISA.

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

(a) la presidenza;

(b) i luoghi di riunione;

(c) la preparazione delle riunioni;

(d) l'ammissione di esperti alle riunioni;

(e) i piani di comunicazione atti a garantire che siano fornite informazioni complete ai membri non partecipanti del consiglio di amministrazione.

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

Tutte le spese di viaggio e di soggiorno sostenute dai membri del consiglio di gestione del programma sono a carico di eu-LISA e l'articolo 10 del suo regolamento interno si applica mutatis mutandis. eu-LISA fornisce un segretariato al consiglio di gestione del programma.

Il gruppo consultivo sull'interoperabilità di cui all'articolo 65 si riunisce regolarmente fino all'entrata in funzione delle componenti dell'interoperabilità. Dopo ciascuna riunione, riferisce al consiglio di gestione del programma. Fornisce la consulenza tecnica a sostegno delle attività del consiglio di gestione del programma e monitora lo stato di preparazione degli Stati membri.

Articolo 53
Responsabilità di eu-LISA in seguito all'entrata in funzione

1. In seguito all'entrata in funzione di ciascuna componente dell'interoperabilità, eu-LISA è responsabile della gestione tecnica dell'infrastruttura centrale e delle interfacce uniformi nazionali. In cooperazione con gli Stati membri, provvede a che in qualsiasi momento siano utilizzate, previa analisi costi/benefici, le migliori tecnologie disponibili. eu-LISA è inoltre responsabile della gestione tecnica dell'infrastruttura di comunicazione di cui agli articoli 6, 12, 17, 25 e 39.

   La gestione tecnica delle componenti dell'interoperabilità consiste nell'insieme dei compiti necessari per garantire il funzionamento delle componenti dell'interoperabilità 24 ore su 24 e 7 giorni su 7 in conformità del presente regolamento e comprende, in particolare, la manutenzione e gli adeguamenti tecnici necessari per garantire che le componenti funzionino a un livello di qualità tecnica soddisfacente, specialmente per quanto riguarda i tempi di risposta alle interrogazioni dell'infrastruttura centrale, conformemente alle specifiche tecniche.

2. Fatto salvo l'articolo 17 dello statuto dei funzionari dell'Unione europea, eu-LISA applica a tutti i membri del proprio personale che operano con i dati conservati nelle componenti dell'interoperabilità adeguate norme in materia di segreto professionale o altri obblighi di riservatezza equivalenti. Tale obbligo vincola il personale anche dopo che ha lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

3. eu-LISA sviluppa e mantiene un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati conservati nel servizio comune di confronto biometrico e nell'archivio comune di dati di identità conformemente all'articolo 37.

4. eu-LISA svolge compiti relativi alla formazione sull'uso tecnico delle componenti dell'interoperabilità.

Articolo 54
Responsabilità degli Stati membri

1. Ciascuno Stato membro è responsabile di quanto segue:

   (a) la connessione all'infrastruttura di comunicazione del portale di ricerca europeo e dell'archivio comune di dati di identità;

   (b) l'integrazione dei sistemi e delle infrastrutture nazionali esistenti con il portale di ricerca europeo, il servizio comune di confronto biometrico, l'archivio comune di dati di identità e il rilevatore di identità multiple;

   (c) l'organizzazione, la gestione, il funzionamento e la manutenzione della propria infrastruttura nazionale esistente e della sua connessione alle componenti dell'interoperabilità;

   (d) la gestione e le modalità di accesso al portale di ricerca europeo, all'archivio comune di dati di identità e al rilevatore di identità multiple del personale debitamente autorizzato delle autorità nazionali competenti, quale che sia il tipo di autorizzazione, a norma del presente regolamento, nonché la creazione e l'aggiornamento periodico di un elenco di tale personale con le relative qualifiche;

   (e) l'adozione delle misure legislative di cui all'articolo 20, paragrafo 2, ai fini

dell'accesso all'archivio comune di dati di identità a fini di identificazione;

(f) la verifica manuale delle identità diverse di cui all'articolo 29;

(g) l'attuazione dei requisiti di qualità dei dati nei sistemi di informazione dell'UE e nelle componenti dell'interoperabilità;

(h) la correzione delle carenze riscontrate nella relazione di valutazione della Commissione riguardante la qualità dei dati di cui all'articolo 37, paragrafo 5.

2. Ciascuno Stato membro provvede alla connessione delle rispettive autorità designate di cui all'articolo 4, punto 24, all'archivio comune di dati di identità.

Articolo 54 bis
Responsabilità di Europol

1. Europol provvede al trattamento delle interrogazioni dei dati Europol effettuate tramite il portale di ricerca europeo e adatta di conseguenza la sua interfaccia QUEST ("Querying Europol Systems") per i dati con un livello di protezione minimo.

2. Europol è responsabile della gestione e delle modalità d'uso e di accesso al portale di ricerca europeo e all'archivio comune di dati di identità da parte del suo personale debitamente autorizzato, a norma del presente regolamento, nonché della creazione e dell'aggiornamento periodico di un elenco di tale personale con le relative qualifiche.

Articolo 55
Responsabilità dell'unità centrale ETIAS

L'unità centrale ETIAS è responsabile di quanto segue:

(a) la verifica manuale delle identità diverse di cui all'articolo 29;

(b) la rilevazione di identità multiple tra i dati conservati nel VIS, nell'Eurodac e nel SIS di cui all'articolo 59.

CAPO IX
Disposizioni finali

Articolo 56
Relazioni e statistiche

1. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi al portale di ricerca europeo, unicamente per elaborare relazioni e statistiche e senza che sia possibile l'identificazione individuale:

(a) numero di interrogazioni per utente del profilo ESP;

(b) – (non pertinente).

2. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati

relativi all'archivio comune di dati di identità, unicamente per elaborare relazioni e statistiche e senza che sia possibile l'identificazione individuale:

(a) numero di interrogazioni ai fini degli articoli 20, 21 e 22;

(b) cittadinanza, sesso e anno di nascita della persona interessata;

(c) tipo del documento di viaggio e codice a tre lettere del paese di rilascio;

(d) numero di interrogazioni effettuate con dati biometrici e senza.

3. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi al rilevatore di identità multiple, unicamente per elaborare relazioni e statistiche e senza che sia possibile l'identificazione individuale:

(a) cittadinanza, sesso e anno di nascita della persona interessata;

(b) tipo del documento di viaggio e codice a tre lettere del paese di rilascio;

(c) numero di interrogazioni effettuate con dati biometrici e senza;

(d) numero di ciascun tipo di collegamento.

4. Il personale debitamente autorizzato dell'Agenzia europea della guardia di frontiera e costiera istituita con regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio[64] ha accesso alla consultazione dei dati di cui ai paragrafi 1, 2 e 3 ai fini dell'esecuzione delle analisi del rischio e delle valutazioni delle vulnerabilità di cui agli articoli 11 e 13 di tale regolamento.

5. Ai fini del paragrafo 1, eu-LISA conserva i dati ivi previsti nell'archivio centrale di relazioni e statistiche di cui al capo VII. I dati figuranti nell'archivio non consentono l'identificazione delle persone fisiche ma permettono alle autorità di cui al paragrafo 1 di ricavare relazioni e dati statistici personalizzabili al fine di migliorare l'efficienza delle verifiche di frontiera, assistere le autorità nel trattamento delle domande di visto e sostenere politiche migratorie dell'Unione basate su dati concreti.

Articolo 57
Periodo transitorio per l'uso del portale di ricerca europeo

Per un periodo di due anni a partire dall'entrata in funzione del portale di ricerca europeo gli obblighi di cui all'articolo 7, paragrafi 2 e 4, non si applicano e l'uso del portale è facoltativo.

Articolo 58
Periodo transitorio per l'applicazione delle disposizioni sull'accesso all'archivio comune di dati di identità a fini di contrasto

L'articolo 22 si applica a partire dalla data di entrata in funzione di cui all'articolo 62, paragrafo 1.

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

Articolo 59
Periodo transitorio per il rilevatore di identità multiple

1. Per un periodo di un anno dopo che eu-LISA comunica il completamento del collaudo di cui all'articolo 62, paragrafo 1, lettera b), in relazione al rilevatore di identità multiple e fino all'entrata in funzione di quest'ultimo, l'unità centrale ETIAS di cui [all'articolo 33(a) del regolamento (UE) 2016/1624] è competente per effettuare le rilevazioni di identità multiple tra i dati conservati nel VIS, nell'Eurodac e nel SIS. Le rilevazioni di identità multiple sono effettuate usando esclusivamente i dati biometrici conformemente all'articolo 27, paragrafo 2.

2. Qualora dall'interrogazione risultino uno o più riscontri positivi e i dati di identità dei fascicoli oggetto del collegamento siano identici o simili, è creato un collegamento bianco conformemente all'articolo 33.

   Qualora dall'interrogazione risultino uno o più riscontri positivi e i dati di identità dei fascicoli oggetto del collegamento non possano essere considerati simili, è creato un collegamento giallo conformemente all'articolo 30 e si applica la procedura di cui all'articolo 29.

   Qualora risultino più riscontri positivi è creato un collegamento tra tutti i dati per i quali è emerso un riscontro positivo.

3. Qualora sia creato un collegamento giallo conformemente al paragrafo 3, il rilevatore di identità multiple permette all'unità centrale ETIAS di consultare i dati di identità presenti nei vari sistemi di informazione.

4. Qualora sia creato un collegamento con una segnalazione nel SIS diversa da una segnalazione a fini di respingimento o da una segnalazione relativa a un documento di viaggio segnalato come smarrito, rubato o invalidato di cui, rispettivamente, all'articolo 24 del regolamento sul SIS nel settore delle verifiche di frontiera e all'articolo 38 del regolamento sul SIS nel settore dell'attività di contrasto, il rilevatore di identità multiple permette all'ufficio SIRENE dello Stato membro che ha creato la segnalazione di consultare i dati di identità presenti nei vari sistemi di informazione.

5. L'unità centrale ETIAS o l'ufficio SIRENE dello Stato membro che ha creato la segnalazione accede ai dati contenuti nel fascicolo di conferma dell'identità ed esamina le identità diverse, aggiorna il collegamento conformemente agli articoli da 31 a 33 e lo aggiunge al fascicolo di conferma dell'identità.

6. Se necessario eu-LISA fornisce assistenza all'unità centrale ETIAS ai fini dello svolgimento delle rilevazioni di identità multiple di cui al presente articolo.

Articolo 60
Spese

1. Le spese sostenute per l'istituzione e il funzionamento del portale di ricerca europeo, del servizio comune di confronto biometrico, dell'archivio comune di dati di identità e del rilevatore di identità multiple sono a carico del bilancio generale dell'Unione.

2. Le spese sostenute per l'integrazione delle esistenti infrastrutture nazionali e la loro connessione alle interfacce nazionali uniformi nonché per ospitare le interfacce nazionali uniformi sono a carico del bilancio generale dell'Unione.

   Sono escluse le seguenti spese:

(a) l'ufficio di gestione di progetto degli Stati membri (riunioni, missioni, uffici);

(b) l'hosting dei sistemi IT nazionali (spazio, implementazione, elettricità, impianti di raffreddamento);

(c) la gestione di sistemi IT nazionali (operatori e contratti di assistenza);

(d) la progettazione, lo sviluppo, l'implementazione, il funzionamento e la manutenzione di reti di comunicazione nazionali.

3. Le spese sostenute dalle autorità designate di cui all'articolo 4, punto 24, sono a carico, rispettivamente, di ciascuno Stato membro e di Europol. Le spese per connettere all'archivio comune di dati di identità le autorità designate sono a carico, rispettivamente, di ciascuno Stato membro e di Europol.

Articolo 61
Comunicazioni

1. Gli Stati membri comunicano a eu-LISA i nominativi delle rispettive autorità di cui agli articoli 7, 20, 21 e 26 che possono usare il portale di ricerca europeo, l'archivio comune di dati di identità e rilevatore di identità multiple o accedervi.

Entro tre mesi dall'entrata in funzione di ciascuna componente dell'interoperabilità a norma dell'articolo 62, un elenco consolidato di tali autorità è pubblicato nella *Gazzetta ufficiale dell'Unione europea*. Qualora l'elenco subisca modifiche, eu-LISA pubblica una volta all'anno un elenco consolidato aggiornato.

2. eu-LISA comunica alla Commissione il positivo completamento del collaudo di cui all'articolo 62, paragrafo 1, lettera b).

3. L'unità centrale ETIAS comunica alla Commissione il positivo completamento della misura transitoria di cui all'articolo 59.

4. La Commissione mette a disposizione degli Stati membri e del pubblico le informazioni di cui al paragrafo 1, tenendo costantemente aggiornata la pagina web.

Articolo 62
Entrata in funzione

1. La Commissione decide la data a partire dalla quale ciascuna componente dell'interoperabilità entra in funzione una volta che:

(a) siano state adottate le misure di cui all'articolo 8, paragrafo 2, all'articolo 9, paragrafo 7, all'articolo 28, paragrafi 5 e 6, all'articolo 37, paragrafo 4, all'articolo 38, paragrafo 4, all'articolo 39, paragrafo 5, e all'articolo 44, paragrafo 5;

(b) eu-LISA abbia dichiarato il positivo completamento di un collaudo generale della pertinente componente dell'interoperabilità, che deve essere effettuato da eu-LISA stessa in cooperazione con gli Stati membri;

(c) eu-LISA abbia convalidato le necessarie disposizioni tecniche e giuridiche per raccogliere e trasmettere i dati di cui all'articolo 8, paragrafo 1, e agli articoli 13, 19, 34 e 39 e le abbia comunicate alla Commissione;

(d) gli Stati membri abbiano comunicato alla Commissione le informazioni previste all'articolo 61, paragrafo 1;

(e) in relazione al rilevatore di identità multiple, l'unità centrale ETIAS abbia comunicato alla Commissione le informazioni previste all'articolo 61, paragrafo 3.

2. La Commissione informa il Parlamento europeo e il Consiglio dell'esito del collaudo effettuato in base al paragrafo 1, lettera b).

3. La decisione della Commissione di cui al paragrafo 1 è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

4. Gli Stati membri ed Europol iniziano a utilizzare le componenti dell'interoperabilità a decorrere dalla data stabilita dalla Commissione ai sensi del paragrafo 1.

Articolo 63
Esercizio della delega

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

2. Il potere di adottare gli atti delegati di cui all'articolo 8, paragrafo 2, e all'articolo 9, paragrafo 7, è conferito alla Commissione per un periodo indeterminato a decorrere dal [*data di entrata in vigore del presente regolamento*].

3. La delega di potere di cui all'articolo 8, paragrafo 2, e all'articolo 9, paragrafo 7, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

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

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

6. L'atto delegato adottato ai sensi dell'articolo 8, paragrafo 2, e dell'articolo 9, paragrafo 7, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di [due mesi] dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di [due mesi] su iniziativa del Parlamento europeo o del Consiglio.

Articolo 64
Procedura di comitato

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

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

Articolo 65
Gruppo consultivo

eu-LISA istituisce un gruppo consultivo che le fornisca consulenza tecnica relativa all'interoperabilità, in particolare nel contesto della preparazione del programma di lavoro annuale e della relazione annuale di attività. In fase di progettazione e di sviluppo degli strumenti di interoperabilità si applica l'articolo 52, paragrafi da 4 a 6.

Articolo 66
Formazione

eu-LISA svolge compiti relativi all'offerta di formazione sull'uso tecnico delle componenti dell'interoperabilità a norma del regolamento (UE) n. 1077/2011.

Articolo 67
Manuale pratico

La Commissione, in stretta cooperazione con gli Stati membri, eu-LISA e altre agenzie pertinenti, mette a disposizione un manuale pratico per l'implementazione e la gestione delle componenti dell'interoperabilità. Il manuale pratico fornisce orientamenti tecnici e operativi, raccomandazioni e migliori prassi. La Commissione adotta il manuale pratico sotto forma di raccomandazione.

Articolo 68
Monitoraggio e valutazione

1. eu-LISA provvede affinché siano istituite procedure per monitorare lo sviluppo delle componenti dell'interoperabilità rispetto agli obiettivi relativi alla pianificazione e ai costi, nonché per monitorare il funzionamento delle componenti dell'interoperabilità rispetto agli obiettivi prefissati in termini di risultati tecnici, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

2. Entro [*sei mesi dopo l'entrata in vigore del presente regolamento* — OPOCE: sostituire con la data effettiva] e successivamente ogni sei mesi durante la fase di sviluppo delle componenti dell'interoperabilità, eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sulla situazione dello sviluppo delle componenti dell'interoperabilità. Una volta che lo sviluppo è completato, è presentata al Parlamento europeo e al Consiglio una relazione che illustra nel dettaglio il modo in cui sono stati conseguiti gli obiettivi, in particolare quelli relativi alla pianificazione e ai costi, giustificando eventuali scostamenti.

3. Ai fini della manutenzione tecnica, eu-LISA ha accesso alle informazioni necessarie riguardanti le operazioni di trattamento dei dati effettuate nelle componenti dell'interoperabilità.

4. Quattro anni dopo l'entrata in funzione di ciascuna componente dell'interoperabilità, e successivamente ogni quattro anni, eu-LISA presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico delle componenti dell'interoperabilità, compresa la loro sicurezza.

5. Un anno dopo ogni relazione di eu-LISA la Commissione effettua una valutazione globale delle componenti, che comprende:

(a) una valutazione dell'applicazione del presente regolamento;

(b) un'analisi dei risultati conseguiti in relazione agli obiettivi prefissati e dell'incidenza sui diritti fondamentali;

(c) una valutazione della perdurante validità dei principi di base delle componenti dell'interoperabilità;

(d) una valutazione della sicurezza delle componenti dell'interoperabilità;

(e) una valutazione delle eventuali implicazioni, incluso qualsiasi impatto sproporzionato sul flusso di traffico ai valichi di frontiera, e di quelle aventi un impatto sul bilancio dell'Unione.

Le valutazioni comprendono le necessarie raccomandazioni. La Commissione trasmette la relazione di valutazione al Parlamento europeo, al Consiglio, al garante europeo della protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali istituita con regolamento (CE) n. 168/2007 del Consiglio[65].

6. Gli Stati membri ed Europol comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 4 e 5. Tali informazioni non mettono a repentaglio i metodi di lavoro né comprendono indicazioni sulle fonti, sui membri del personale o sulle indagini delle autorità designate.

7. eu-LISA comunica alla Commissione le informazioni necessarie per redigere le valutazioni di cui al paragrafo 5.

8. Nel rispetto delle disposizioni del diritto nazionale relative alla pubblicazione di informazioni sensibili, ciascuno Stato membro ed Europol predispongono relazioni annuali sull'efficacia dell'accesso ai dati conservati nell'archivio comune di dati di identità a fini di contrasto, in cui figurino informazioni e statistiche su quanto segue:

(a) lo scopo esatto della consultazione, compreso il tipo di reato di terrorismo o altro reato grave;

(b) i fondati motivi addotti per il sospetto fondato che l'autore presunto o effettivo oppure la vittima rientri nel campo di applicazione del regolamento;

(c) il numero delle richieste di accesso all'archivio comune di dati di identità a fini di contrasto;

(d) 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 il punto di accesso centrale 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.

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

Articolo 69
Entrata in vigore e applicazione

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

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

Fatto a Strasburgo, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati

1.3. Natura della proposta/iniziativa

1.4. Obiettivi

1.5. Motivazione della proposta/iniziativa

1.6. Durata e incidenza finanziaria

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

3.2.2. Incidenza prevista sugli stanziamenti operativi

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce l'interoperabilità tra i sistemi di informazione dell'Unione europea per la sicurezza, le frontiere e la gestione della migrazione.

.

1.2. Settore/settori interessati

Affari interni (titolo 18)

1.3. Natura della proposta/iniziativa

X La proposta/iniziativa riguarda **una nuova azione**

☐ La proposta/iniziativa riguarda **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[66]

☐ La proposta/iniziativa riguarda **la proroga di un'azione esistente**

☐ La proposta/iniziativa riguarda **un'azione riorientata verso una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi strategici pluriennali della Commissione oggetto della proposta/iniziativa

Gestione delle frontiere – salvare vite umane e rendere sicure le frontiere esterne

Le componenti dell'interoperabilità consentono di sfruttare meglio le informazioni figuranti negli attuali sistemi dell'UE per la sicurezza, le frontiere e la gestione della migrazione. Sostanzialmente permettono di evitare che una persona sia registrata in più sistemi con identità diverse. Attualmente è possibile identificare in modo univoco una persona solo all'interno di un dato sistema ma non trasversalmente in tutti i sistemi. Questa situazione può portare a decisioni erronee delle autorità o essere sfruttata dai viaggiatori in mala fede che vogliono nascondere la propria vera identità.

Migliore scambio delle informazioni

Le misure proposte consentono ai servizi di contrasto di accedere agevolmente a tali dati, ma entro limiti ben determinati. Contrariamente ad oggi, ci sarà un unico insieme di condizioni anziché condizioni diverse a seconda dei dati da consultare.

1.4.2. Obiettivi specifici e obiettivo specifico n. [ ]

L'istituzione delle componenti dell'interoperabilità persegue i seguenti obiettivi generali:

(a) migliorare la gestione delle frontiere esterne;

(b) contribuire a prevenire e combattere l'immigrazione irregolare;

[66] A norma dell'articolo 54, paragrafo 2, lettera a) o b), del regolamento finanziario.

(c) contribuire ad assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, inclusi il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri.

Gli obiettivi dell'interoperabilità sono realizzati:

a) garantendo la corretta identificazione delle persone;

b) contribuendo a contrastare la frode di identità;

c) migliorando e armonizzando i requisiti di qualità dei dati dei diversi sistemi di informazione dell'UE;

d) agevolando gli Stati membri nell'attuazione tecnica e operativa degli attuali e futuri sistemi di informazione dell'UE;

e) rafforzando, semplificando e rendendo più uniformi le condizioni di sicurezza e protezione dei dati che disciplinano i diversi sistemi di informazione dell'UE;

f) semplificando e rendendo più uniformi le condizioni di accesso all'EES, al VIS, all'ETIAS e all'Eurodac a fini di contrasto;

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

Attività ABM/ABB interessate

Sicurezza e tutela delle libertà: sicurezza interna

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

Gli obiettivi generali della presente iniziativa derivano da due obiettivi basati sul trattato:

1. migliorare la gestione delle frontiere esterne dello spazio Schengen, sulla base dell'agenda europea sulla migrazione e delle comunicazioni successive, tra cui la comunicazione sul mantenimento e sul rafforzamento dello spazio Schengen;

2. contribuire alla sicurezza interna dell'Unione europea, sulla base dell'agenda europea sulla sicurezza e dei lavori della Commissione per un'autentica ed efficace Unione della sicurezza.

Gli obiettivi strategici specifici della presente iniziativa sull'interoperabilità sono i seguenti:

Gli obiettivi specifici della presente proposta sono:

1. far sì che gli utenti finali, in particolare le guardie di frontiera, le autorità di contrasto, gli operatori dei servizi per l'immigrazione e le autorità giudiziarie possano accedere rapidamente e in modo continuato, sistematico e controllato alle informazioni di cui hanno bisogno per svolgere i loro compiti;

2. fornire una soluzione per individuare le identità multiple collegate a uno stesso insieme di dati biometrici, al duplice scopo di garantire la corretta identificazione delle persone in buona fede e combattere la frode di identità;

3. facilitare le verifiche di identità dei cittadini di paesi terzi presenti sul territorio di uno Stato membro da parte di autorità di polizia;

4. agevolare e semplificare l'accesso delle autorità di contrasto ai sistemi di informazione estranei al settore del contrasto a livello dell'UE a fini di prevenzione, indagine, accertamento o perseguimento di reati gravi e del terrorismo.

Per raggiungere l'obiettivo specifico 1 sarà sviluppato un portale di ricerca europeo (ESP).

Per raggiungere l'obiettivo specifico 2 sarà messo a punto un rilevatore di identità multiple (MID), affiancato da un archivio comune di dati di identità (CIR) e da un servizio comune di confronto biometrico (BMS comune).

Per raggiungere l'obiettivo specifico 3 i funzionari autorizzati potranno accedere al CIR a fini di identificazione.

Per raggiungere l'obiettivo 4 il CIR conterrà una funzione di segnalazione "hit/no hit" che permetterà un approccio a due fasi per accedere ai sistemi di gestione delle frontiere a fini di contrasto.

Oltre a queste quattro componenti dell'interoperabilità, contribuiranno a raggiungere gli obiettivi descritti alla sezione 1.4.2 anche la creazione e governance del formato universale dei messaggi (UMF), quale standard dell'UE per lo sviluppo dei sistemi di informazione nel settore Giustizia e affari interni, e l'istituzione di un archivio centrale di relazioni e statistiche (CRRS).

1.4.4. Indicatori di risultato e di incidenza

Precisare gli indicatori che permettono di seguire l'attuazione della proposta/iniziativa.

Ciascuna delle misure proposte richiede dapprima lo sviluppo della componente e poi la sua manutenzione e messa in funzione.

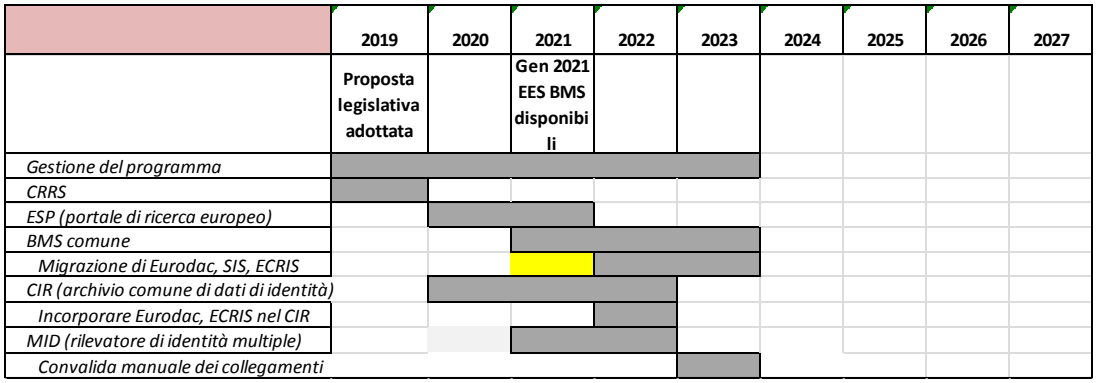
Durante la fase di sviluppo

Lo sviluppo di ciascuna componente inizierà una volta soddisfatti i prerequisiti, ovvero dopo che i colegislatori avranno adottato la proposta legislativa e quando sussisteranno i prerequisiti tecnici essenziali, giacché alcune componenti potranno essere elaborate solo dopo che altre componenti sono state realizzate.

Obiettivo specifico: operatività entro la data prevista

Entro la fine del 2017 la proposta è trasmessa ai colegislatori per adozione. Basandosi sulla tempistica di altre proposte si presume che l'iter di adozione sarà completato nel corso del 2018.

Partendo da questo presupposto, l'inizio del periodo di sviluppo è stato fissato all'inizio del 2019 (= T0), che funge da punto di riferimento per conteggiare le scadenze successive, senza date assolute. Se i colegislatori adotteranno la proposta più tardi, l'intero calendario slitterà conseguentemente. D'altro canto, per completare il CIR e il MID dovrà prima essere disponibile il BMS comune. La durata della fase di sviluppo è indicata nel grafico seguente:



(la casella in giallo riguarda un compito specifico relativo a Eurodac).

- Archivio centrale di relazioni e statistiche (CRRS): termine previsto: T0 + 12 mesi (2019-2020)

- Portale di ricerca europeo (ESP): termine previsto: T0 + 36 mesi (2019-2021)

- Il servizio comune di confronto biometrico (BMS comune) è creato prima per realizzare il sistema di ingressi/uscite (EES). Una volta conseguita questa tappa, le applicazioni che useranno il BMS comune dovranno essere aggiornate e i dati contenuti nel sistema automatizzato di identificazione dattiloscopica (AFIS) del SIS, nell'AFIS Eurodac e i dati del sistema ECRIS-TCN dovranno migrare nel BMS comune. Il completamento è previsto per la fine del 2023.

- L'archivio comune di dati di identità (CIR) è creato durante l'attuazione dell'EES. Una volta completato l'EES, i dati dell'Eurodac e dell'ECRIS saranno incorporati nel CIR. Il completamento è previsto per la fine del 2022 (disponibilità del BMS comune + 12 mesi).

- Il rilevatore di identità multiple (MID) è creato una volta che il CIR sarà entrato in funzione. Il completamento è previsto per la fine del 2022 (disponibilità del BMS comune + 24 mesi), ma per un certo periodo molte risorse saranno impegnate a convalidare i collegamenti tra le identità proposti dal MID. Ogni collegamento dovrà essere convalidato manualmente. Questo processo durerà fino alla fine del 2023.

La messa in funzione inizia una volta completata la fase di sviluppo.

Messa in funzione

Gli indicatori correlati a ciascun obiettivo specifico di cui al punto 1.4.3 sono i seguenti:

1. Obiettivo specifico: accesso rapido, continuato e sistematico alle fonti di dati autorizzate

- Numero di casi eseguiti (= numero di ricerche che possono essere gestite dall'ESP) per periodo di tempo.

- Numero di ricerche gestite dall'ESP rispetto al numero totale di ricerche (tramite l'ESP e direttamente tramite i sistemi) per periodo di tempo.

2. Obiettivo specifico: rilevare le identità multiple

- Numero di identità collegate a uno stesso insieme di dati biometrici rispetto al numero di identità rilevate con dati anagrafici per periodo di tempo.

- Numero di casi di frode di identità rilevati rispetto al numero di identità oggetto di collegamento e al numero totale di identità per periodo di tempo.

3. Obiettivo specifico: facilitare l'identificazione dei cittadini di paesi terzi

- Numero di controlli di identificazione effettuati rispetto al numero totale di operazioni per periodo di tempo.

4. Obiettivo specifico: semplificare l'accesso a fini di contrasto alle fonti di dati autorizzate

- Numero di accessi "fase 1" (= verifica della presenza di dati) a fini di contrasto per periodo di tempo.

- Numero di accessi "fase 2" (= effettiva consultazione di dati dei pertinenti sistemi dell'UE) a fini di contrasto per periodo di tempo.

5. Obiettivo aggiuntivo e trasversale: migliorare la qualità dei dati e il loro utilizzo per una migliore elaborazione delle politiche

- Presentazione periodica di relazioni di controllo della qualità dei dati.

- Numero di apposite richieste di informazioni statistiche per periodo di tempo.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine

Come dimostrato nella valutazione d'impatto che accompagna la presente proposta legislativa , le componenti proposte sono necessarie per realizzare l'interoperabilità:

• Per conseguire l'obiettivo di fornire agli utenti autorizzati un accesso rapido, continuato, sistematico e controllato ai sistemi di informazione pertinenti, è opportuno creare un portale di ricerca europeo (ESP) basato su un servizio comune di

confronto biometrico (BMS comune) che permetta l'interrogazione di tutte le banche dati;

• Per conseguire l'obiettivo di facilitare le verifiche di identità dei cittadini di paesi terzi presenti sul territorio di uno Stato membro da parte di funzionari autorizzati, è opportuno istituire un archivio comune di dati di identità (CIR) contenente l'insieme minimo di dati di identificazione e basato sul BMS comune.

• Per conseguire l'obiettivo di rilevare le identità multiple collegate a uno stesso insieme di dati biometrici, al duplice scopo di facilitare le verifiche di identità dei viaggiatori in buona fede e combattere la frode d'identità, è opportuno istituire un rilevatore di identità multiple (MID) contenente i collegamenti tra le identità multiple nei vari sistemi.

• Per conseguire l'obiettivo di agevolare e semplificare l'accesso delle autorità di contrasto ai sistemi di informazione estranei al settore del contrasto a fini di prevenzione, indagine, accertamento o perseguimento di reati gravi e del terrorismo, è opportuno inserire nel CIR una funzione di segnalazione "hit/no hit".

Poiché tutti gli obiettivi devono essere conseguiti, la soluzione completa è la combinazione dell'ESP, del CIR (con la funzione di segnalazione "hit/no hit") e del MID, basando tutte queste componenti sul BMS comune.

1.5.2. Valore aggiunto dell'intervento dell'Unione europea (che può derivare da diversi fattori, tra cui per esempio un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto si intende per "valore aggiunto dell'intervento dell'Unione" il valore derivante dall'intervento dell'Unione che si aggiunge al valore che sarebbe altrimenti stato generato da un singolo Stato membro.

È necessario intervenire a livello europeo in quanto i sistemi che si propone di rendere interoperabili sono usati da più Stati membri (tutti gli Stati membri nel caso dell'Eurodac e tutti gli Stati membri che fanno parte dello spazio Schengen nel caso dell'EES, del VIS, dell'ETIAS e del SIS). Per definizione, un'azione non può essere adottata a un altro livello.

Il principale valore aggiunto atteso è di eliminare i casi di frode di identità, mappare i casi in cui una persona ha usato identità diverse per entrare nell'UE ed evitare che persone in buona fede siano confuse con persone in malafede aventi lo stesso nome. Un ulteriore valore aggiunto è che l'interoperabilità proposta consente un'attuazione e una manutenzione più agevoli dei sistemi IT su larga scala dell'UE. Per i servizi di contrasto, le misure proposte dovrebbero portare a un accesso più frequente e con esito positivo a dati specifici contenuti nei sistemi IT su larga scala dell'UE. A livello operativo, la qualità dei dati può essere mantenuta e migliorata soltanto se è monitorata. Inoltre, ai fini dell'elaborazione delle politiche e del processo decisionale, occorre rendere possibili interrogazioni ad hoc di dati anonimizzati.

La valutazione d'impatto contiene un'analisi costi/benefici. Tenuto conto solo dei benefici quantificabili, si possono ragionevolmente attendere circa 77,5 milioni di EUR all'anno di benefici, che andrebbero principalmente agli Stati membri. Tali benefici derivano essenzialmente da:

- costi ridotti per modificare le applicazioni nazionali quando il sistema centrale diventa operativo (stimati a 6 milioni di EUR all'anno per dipartimenti informatici dei diversi Stati membri);

- risparmi di costi derivanti dall'aver un BMS comune anziché un BMS per ciascun sistema centrale contenente dati biometrici (stimati a 1,5 milioni di EUR all'anno e un risparmio una tantum di 8 milioni di EUR per eu-LISA);

- costi risparmiati per l'identificazione delle identità multiple rispetto alla situazione senza i mezzi proposti. Si tratterebbe di un risparmio di almeno 50 milioni di EUR all'anno per le amministrazioni degli Stati membri incaricate della gestione delle frontiere, della migrazione e dell'attività di contrasto;

- costi di formazione risparmiati per un ampio gruppo di utenti finali rispetto alla situazione in cui è necessaria una formazione su base periodica (stimati a 20 milioni di EUR all'anno per le amministrazioni degli Stati membri incaricate della gestione delle frontiere, della migrazione e dell'attività di contrasto).

1.5.3. Insegnamenti tratti da esperienze analoghe

L'esperienza acquisita con lo sviluppo del sistema d'informazione Schengen di seconda generazione (SIS II) e del sistema d'informazione visti (VIS) ha permesso di trarre i seguenti insegnamenti:

1. Come possibile salvaguardia contro il superamento dei costi e i ritardi derivanti dal cambiamento dei requisiti, un nuovo sistema d'informazione nel settore della libertà, sicurezza e giustizia, in particolare se comprende un sistema IT su larga scala, non dovrebbe essere sviluppato prima che siano stati definitivamente adottati gli strumenti giuridici che ne stabiliscono le finalità, l'ambito di applicazione, le funzioni e le particolarità tecniche.

2. Per il SIS II e il VIS, gli sviluppi nazionali negli Stati membri avrebbero potuto essere cofinanziati dal Fondo per le frontiere esterne, ma questa non era una condizione obbligatoria. Di conseguenza non è stato possibile avere una visione generale del livello di avanzamento in quegli Stati membri che non avevano previsto le rispettive attività nella loro programmazione pluriennale o che non avevano una programmazione abbastanza precisa. Si propone pertanto che la Commissione rimborsi tutti i costi di integrazione sostenuti dagli Stati membri, per poter controllare l'avanzamento di questi sviluppi.

3. Al fine di facilitare il coordinamento generale dell'attuazione, tutti gli scambi di messaggi proposti tra i sistemi nazionali e i sistemi centrali sfrutteranno le reti e l'interfaccia uniforme nazionale esistenti.

1.5.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

Compatibilità con il vigente quadro finanziario pluriennale

Il regolamento ISF-Frontiere è lo strumento finanziario in cui è stato inserito il bilancio per l'attuazione dell'iniziativa sull'interoperabilità.

Esso prevede, all'articolo 5, paragrafo 5, lettera b), che 791 milioni di EUR siano attuati tramite un programma per lo sviluppo di sistemi informatici basati su sistemi esistenti e/o nuovi a sostegno della gestione dei flussi migratori attraverso le frontiere esterne previa adozione dei pertinenti atti legislativi dell'Unione e nel rispetto delle condizioni di cui all'articolo 15, paragrafo 5. Di questi 791 milioni di EUR, 480,2 milioni sono riservati allo sviluppo dell'EES, 210 milioni per l'ETIAS e 67,9 milioni per la revisione del SIS II. Quel che resta (32,9 milioni di EUR) va riattribuito secondo i meccanismi dell'ISF-Frontiere. Per il rimanente periodo coperto dal

quadro finanziario pluriennale attuale, la presente proposta necessita di una dotazione pari a 32,1 milioni di EUR, vale a dire un importo rientrante nella dotazione restante.

La proposta attuale richiede una dotazione totale di 424,7 milioni di EUR (inclusa la rubrica 5) per il periodo 2019-2027. L'attuale quadro finanziario pluriennale copre solo il biennio 2019-2020. Tuttavia i costi sono stati stimati fino al 2027 incluso per fornire una panoramica informata delle conseguenze della presente proposta e senza compromettere il prossimo quadro finanziario pluriennale.

La dotazione richiesta per i nove anni ammonta a 424,7 milioni di EUR e copre le seguenti voci:

(1) 136,3 milioni di EUR per gli Stati membri per coprire le modifiche dei loro sistemi nazionali necessarie per utilizzare le componenti dell'interoperabilità e la NUI fornita da eu-LISA, e una dotazione per la formazione della numerosa comunità di utenti finali. Non vi è incidenza sull'attuale quadro finanziario pluriennale giacché il finanziamento è previsto a partire dal 2021;

(2) 4,8 milioni di EUR per l'Agenzia europea della guardia di frontiera e costiera per ospitare un gruppo di specialisti che per un anno (2023) convalideranno i collegamenti tra identità quando il MID diventerà operativo. Le attività del gruppo possono essere associate alla disambiguazione di identità quale attribuita all'Agenzia europea della guardia di frontiera e costiera nel quadro della proposta ETIAS. Non vi è incidenza sull'attuale quadro finanziario pluriennale giacché il finanziamento è previsto a partire dal 2021;

(3) 48,9 milioni di EUR per Europol per coprire l'aggiornamento dei suoi sistemi informatici per il volume di messaggi da trattare e l'aumento dei livelli di prestazione. Le componenti dell'interoperabilità saranno usate dall'ETIAS per consultare i dati Europol. Tuttavia l'attuale capacità di trattamento delle informazioni di Europol non è adeguata ai grandi volumi (in media 100 000 interrogazioni al giorno) e ai ridotti tempi di risposta. 9,1 milioni di EUR sono spesi nell'ambito dell'attuale quadro finanziario pluriennale;

(4) 2,0 milioni di EUR per CEPOL per coprire la preparazione e la realizzazione della formazione per il personale operativo. 0,1 milioni di EUR sono previsti per il 2020;

(5) 225,0 milioni di EUR per eu-LISA per coprire il costo totale per lo sviluppo del programma che realizza le cinque componenti dell'interoperabilità (68,3 milioni di EUR), i costi di manutenzione a partire dal momento in cui le componenti sono realizzate fino al 2027 (56,1 milioni di EUR), una dotazione specifica di 25,0 milioni di EUR per la migrazione dei dati dai sistemi esistenti verso il BMS comune e i costi aggiuntivi per l'aggiornamento della NUI, la rete, la formazione e le riunioni. Una dotazione specifica di 18,7 milioni di EUR copre i costi per aggiornare e far funzionare l'ECRIS-TCN in modalità alta disponibilità a partire dal 2022. Sull'importo totale, 23,0 milioni di EUR sono spesi nell'ambito dell'attuale quadro finanziario pluriennale;

(6) 7,7 milioni di EUR per la DG HOME per coprire un aumento limitato del personale e i relativi costi durante il periodo di sviluppo delle diverse componenti, giacché la Commissione avrà la responsabilità del comitato che si occupa del formato UMF. Tale dotazione, che rientra nella rubrica 5, non è a carico del bilancio dell'ISF. Per informazione 2,0 milioni di EUR sono dovuti per il periodo 2019-2020.

Compatibilità con iniziative precedenti

La presente iniziativa è compatibile con quanto segue:

Nell'aprile 2016 la Commissione ha presentato la comunicazione "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza" al fine di affrontare una serie di problemi strutturali connessi ai sistemi di informazione. Tre azioni hanno fatto seguito:

In primo luogo, la Commissione ha adottato misure per rafforzare e massimizzare i benefici dei sistemi di informazione esistenti. Nel dicembre 2016 la Commissione ha adottato proposte per l'ulteriore rafforzamento dell'attuale sistema d'informazione Schengen (SIS). Nel frattempo, a seguito della proposta della Commissione del maggio 2016, sono stati accelerati i negoziati per la revisione della base giuridica per l'Eurodac, la banca dati dell'UE per le impronte digitali dei richiedenti asilo. Inoltre, è attualmente in fase di preparazione una proposta per una nuova base giuridica per il sistema di informazione visti (VIS), che sarà presentata nel secondo trimestre del 2018.

In secondo luogo, la Commissione ha proposto ulteriori sistemi d'informazione per colmare le lacune individuate nell'architettura di gestione dei dati dell'UE. I negoziati sulla proposta della Commissione dell'aprile 2016 per l'istituzione di un sistema di ingressi/uscite (EES)[67] - per migliorare le procedure di verifica di frontiera sui cittadini di pesi terzi che si recano nell'UE - si sono rapidamente conclusi nel luglio 2017, grazie al raggiungimento di un accordo politico tra i colegislatori confermato poi dal Parlamento europeo nell'ottobre 2017 e adottato formalmente dal Consiglio nel novembre 2017. Nel novembre 2016 la Commissione ha inoltre presentato una proposta per istituire un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)[68], che mira a rafforzare le verifiche di sicurezza sui viaggiatori esenti dall'obbligo del visto permettendo verifiche preventive in materia di migrazione irregolare e sicurezza. La proposta è attualmente in fase di negoziazione da parte dei colegislatori. Nel giugno 2017 è stato proposto il sistema europeo di informazione sui casellari giudiziali per i cittadini di paesi terzi (ECRIS-TCN)[69] al fine di colmare le lacune identificate per quanto riguarda lo scambio di informazioni tra gli Stati membri sui cittadini di paesi terzi condannati.

In terzo luogo, la Commissione ha lavorato all'interoperabilità dei sistemi di informazione, concentrandosi a tal fine sulle quattro opzioni presentate nella comunicazione dell'aprile 2016[70]. Tre delle quattro opzioni sono l'ESP, CIR e il BMS comune. Successivamente è emerso che era necessario operare una distinzione tra il CIR, quale banca dati di identità, e una nuova componente che consentisse di individuare le identità multiple collegate a uno stesso identificatore biometrico (MID). Pertanto le quattro componenti sono ora: l'ESP, il CIR, il MID e il BMS comune.

Sinergia

La sinergia è qui intesa come il vantaggio realizzato sfruttando le soluzioni esistenti ed evitando nuovi investimenti.

Esiste un'importante sinergia tra queste iniziative e lo sviluppo dell'EES e dell'ETIAS.

[67] COM(2016) 194 del 6 aprile 2016.
[68] COM(2016) 731 del 16 novembre 2016.
[69] COM(2017) 344 del 29 giugno 2017.
[70] COM(2016) 205 del 6 aprile 2016.

Per il funzionamento dell'EES viene creato un fascicolo individuale per tutti i cittadini di paesi terzi che entrano nello spazio Schengen per un soggiorno di breve durata. A tal fine, l'attuale sistema di confronto biometrico utilizzato per il VIS, contenente i template delle impronte digitali di tutti i viaggiatori soggetti all'obbligo del visto, sarà esteso ai dati biometrici dei viaggiatori esenti dall'obbligo del visto. Concettualmente il BMS comune è pertanto un'estensione ulteriore del dispositivo di confronto biometrico che sarà creato nell'ambito dell'EES. I template biometrici contenuti nel dispositivo di confronto biometrico del SIS e dell'Eurodac migreranno (migrare è il termine tecnico per indicare il trasferimento di dati da un sistema all'altro) nel dispositivo di confronto biometrico del BMS comune. Stando ai dati dei fornitori, la conservazione in banche dati distinte costa in media 1 EUR per insieme biometrico (potenzialmente gli insiemi di dati sono 200 milioni in totale), mentre il costo medio scende a 0,35 EUR per insieme biometrico se si utilizza una soluzione BMS comune. I costi più elevati per l'hardware necessario per l'enorme volume di dati contrappesano in parte tali vantaggi ma alla fine si stima che il costo del BMS comune sia inferiore del 30% rispetto a quando gli stessi dati sono conservati in più BMS di dimensioni inferiori.

Per il funzionamento dell'ETIAS occorre una componente che permetta di interrogare un insieme di sistemi dell'UE. A tal fine o si usa l'ESP o si deve creare una componente specifica nell'ambito della proposta relativa all'ESP. La proposta sull'interoperabilità consente la creazione di una componente anziché due.

Si ottiene un'altra sinergia anche sfruttando la stessa interfaccia uniforme nazionale (NUI) usata per l'EES e l'ETIAS. La NUI dovrà essere aggiornata ma continuerà ad essere usata.

1.6. Durata e incidenza finanziaria

☐ Proposta/iniziativa di **durata limitata**

– ☐ Proposta/iniziativa in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ Incidenza finanziaria dal AAAA al AAAA

☒ Proposta/iniziativa di **durata illimitata**

– Periodo di sviluppo dal 2019 al 2023 incluso, seguito dal funzionamento su larga scala.

– Si prevede quindi la durata dell'incidenza finanziaria dal 2019 al 2027.

1.7. Modalità di gestione previste[71]

☒ **Gestione diretta** a opera della Commissione

– X a opera dei suoi servizi, compreso il personale delle delegazioni dell'Unione;

– ☐ a opera delle agenzie esecutive.

☒ **Gestione concorrente** con gli Stati membri

☒ **Gestione indiretta** con compiti di esecuzione del bilancio affidati:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e rispettive agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☒ agli organismi di cui agli articoli 208 e 209 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui presentano sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che presentano sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche nel settore della PESC a norma del titolo V del TUE, che devono essere indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

Blocchi	Fase di sviluppo	Fase operativa	Modalità di gestione	Attore
Sviluppo e manutenzione (delle componenti dell'interoperabilità per i sistemi centrali, della formazione all'uso dei sistemi)	X	X	Indiretta	eu-LISA Europol CEPOL

[71] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Blocchi	Fase di sviluppo	Fase operativa	Modalità di gestione	Attore
Migrazione dei dati (migrazione dei template biometrici verso il BMS comune), costi di rete, aggiornamento della NUI, riunioni e formazione	X	X	Indiretta	eu-LISA
Convalida dei collegamenti quando si crea il MID	X	-	Indiretta	Guardia di frontiera e costiera europea
Personalizzazione della NUI, integrazione dei sistemi nazionali e formazione degli utenti finali	X	X	Concorrente (o diretta) (1)	COM + Stati membri

(1) Il presente strumento non contiene importi per la fase operativa.

Il periodo di sviluppo inizia nel 2019 e dura fino alla realizzazione di ciascuna componente, quindi dal 2019 al 2023 (cfr. punto 1.4.4).

1. Gestione diretta a opera della DG HOME: durante il periodo di sviluppo, se necessario, le azioni possono anche essere attuate direttamente dalla Commissione. Ciò potrebbe includere, in particolare, il sostegno finanziario dell'Unione alle attività sotto forma di sovvenzioni (anche alle autorità nazionali degli Stati membri), appalti pubblici e/o rimborso delle spese sostenute dagli esperti esterni.

2. Gestione concorrente: durante la fase di sviluppo gli Stati membri dovranno adattare i loro sistemi nazionali per accedere all'ESP anziché ai singoli sistemi (per i messaggi in uscita dagli Stati membri) e per le modifiche alle risposte delle loro richieste di ricerca (i messaggi in entrata verso gli Stati membri). Sarà inoltre effettuato un aggiornamento dell'attuale NUI attuata per l'EES e l'ETIAS.

3. Gestione indiretta: eu-LISA curerà la parte "sviluppo" di tutti gli elementi IT del progetto, ossia l'interoperabilità delle componenti, l'aggiornamento dell'interfaccia uniforme nazionale (NUI) in ciascuno Stato membro, l'aggiornamento dell'infrastruttura di comunicazione tra i sistemi centrali e le interfacce uniformi nazionali, la migrazione dei template biometrici dagli attuali sistemi di confronto biometrico del SIS e dell'Eurodac verso il BMS comune e la relativa attività di pulizia dei dati.

Durante il periodo operativo eu-LISA eseguirà tutte le attività tecniche legate alla manutenzione delle componenti.

L'Agenzia europea della guardia di frontiera e costiera incorporerà un'ulteriore gruppo incaricato della convalida dei collegamenti dopo l'entrata in funzione del MID. Si tratta di un incarico di durata limitata.

Europol curerà lo sviluppo e la manutenzione dei suoi sistemi per garantire l'interoperabilità con l'ESP e l'ETIAS.

CEPOL elabora e fornisce la formazione ai servizi operativi secondo un approccio di formazione per formatori.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

Disposizioni in materia di monitoraggio e di relazioni per lo sviluppo e la manutenzione di altri sistemi:

1. eu-LISA provvede affinché siano istituite procedure per monitorare lo sviluppo delle componenti dell'interoperabilità rispetto agli obiettivi relativi alla pianificazione e ai costi, nonché per monitorare il funzionamento delle componenti rispetto agli obiettivi prefissati in termini di risultati tecnici, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

2. Entro sei mesi dall'entrata in vigore del regolamento e successivamente ogni sei mesi durante la fase di sviluppo delle componenti, eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sulla situazione dello sviluppo di ciascuna componente. Una volta che lo sviluppo è completato, è presentata al Parlamento europeo e al Consiglio una relazione che illustra nel dettaglio il modo in cui sono stati conseguiti gli obiettivi, in particolare quelli relativi alla pianificazione e ai costi, giustificando eventuali scostamenti.

3. Ai fini della manutenzione tecnica, eu-LISA ha accesso alle informazioni necessarie riguardanti le operazioni di trattamento dei dati effettuate nelle componenti.

4. Quattro anni dopo l'entrata in funzione dell'ultima componente attuata, e successivamente ogni quattro anni, eu-LISA presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico delle componenti.

5. Cinque anni dopo l'entrata in funzione dell'ultima componente attuata e, successivamente ogni quattro anni, la Commissione presenta una valutazione globale e formula le necessarie raccomandazioni. Tale valutazione globale comprende: i risultati ottenuti dalle componenti tenendo conto degli obiettivi dell'interoperabilità, della manutenibilità, delle prestazioni e delle implicazioni finanziarie, e l'impatto sui diritti fondamentali.

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

6. Gli Stati membri e Europol comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai punti 4 e 5 conformemente agli indicatori quantitativi predefiniti dalla Commissione e/o da eu-LISA. Tali informazioni non mettono a repentaglio i metodi di lavoro né comprendono indicazioni sulle fonti, sull'identità dei membri del personale o sulle indagini delle autorità designate.

7. eu-LISA comunica alla Commissione le informazioni necessarie per presentare le valutazioni di cui al punto 5.

8. Nel rispetto delle disposizioni del diritto nazionale relative alla pubblicazione di informazioni sensibili, ciascuno Stato membro ed Europol predispongono una relazione annuale sull'efficacia dell'accesso ai sistemi dell'UE a fini di contrasto, in cui figurino informazioni e statistiche su quanto segue:

- lo scopo esatto della consultazione, compreso il tipo di reato di terrorismo o altro reato grave;

- i fondati motivi addotti per il sospetto fondato che l'autore presunto o effettivo oppure la vittima rientri nel campo di applicazione del regolamento;

- il numero delle richieste di accesso alle componenti a fini di contrasto;

- il numero e il tipo di casi in cui si è giunti a un'identificazione;

- la necessità di trattare casi eccezionali d'urgenza, compresi i casi in cui il punto di accesso centrale non ha confermato l'urgenza dopo la verifica a posteriori.

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

2.2. Sistema di gestione e di controllo

2.2.1. Rischi individuati

I rischi sono quelli collegati al fatto che lo sviluppo informatico delle cinque componenti sia effettuato da un contraente esterno gestito da eu-LISA. I tipici rischi del progetto sono:

1. il rischio che il progetto non sia completato in tempo;

2. il rischio che il progetto non sia completato nel rispetto del bilancio;

3. il rischio che il progetto non sia realizzato appieno.

Il primo rischio è il più importante giacché lo sforamento dei tempi comporta un aumento delle spese in quanto la maggior parte delle spese è legata alla durata: spese di personale, spese di licenza per anno, ecc.

Questi rischi possono essere attenuati applicando tecniche di gestione del progetto, tra cui una riserva per imprevisti nei progetti di sviluppo e personale sufficiente per assorbire picchi di lavoro. Di norma infatti gli sforzi sono stimati ipotizzando un'equa distribuzione del carico di lavoro nel tempo mentre nella realtà si assiste a carichi di lavoro disomogenei che vengono assorbiti da stanziamenti di risorse maggiori.

Il ricorso a un contraente esterno per questo lavoro di sviluppo comporta vari rischi:

1. in particolare, il rischio che il contraente non riesca a stanziare risorse sufficienti per il progetto o che formuli e sviluppi un sistema non abbastanza avanzato;

2. il rischio che il contraente, per ridurre i costi, non rispetti pienamente le tecniche e le metodologie amministrative per gestire progetti IT su larga scala;

3. infine non può essere del tutto escluso il rischio che il contraente sperimenti difficoltà finanziarie per ragioni esterne al progetto.

Questi rischi sono attenuati aggiudicando i contratti in base a criteri di qualità rigorosi, verificando i riferimenti dei contraenti e mantenendo stretti rapporti con i contraenti. Infine, come ultima risorsa, possono essere incluse e applicate, se necessario, penalità rigorose e clausole di risoluzione.

2.2.2. Informazioni riguardanti il sistema di controllo interno istituito

eu-LISA è concepita come centro di eccellenza nel settore dello sviluppo e della gestione di sistemi IT su larga scala. Essa esegue le attività legate allo sviluppo e al

funzionamento delle diverse componenti dell'interoperabilità, compresa la manutenzione dell'interfaccia uniforme nazionale negli Stati membri.

Nella fase di sviluppo tutte le attività di sviluppo saranno svolte da eu-LISA. Tra queste rientrerà la parte "sviluppo" di tutti gli elementi del progetto. I costi correlati all'integrazione dei sistemi negli Stati membri durante lo sviluppo saranno gestiti dalla Commissione in gestione concorrente o tramite sovvenzioni.

Durante la fase operativa, eu-LISA sarà responsabile della gestione tecnica e finanziaria delle componenti usate a livello centrale, in particolare l'aggiudicazione e la gestione dei contratti. La Commissione gestirà i finanziamenti agli Stati membri per le spese relative alle unità nazionali tramite ISF Frontiere (programmi nazionali).

Per evitare ritardi a livello nazionale, prima dell'avvio della fase di sviluppo occorre predisporre una governance efficiente tra tutti i portatori di interessi. La Commissione parte dal presupposto che l'architettura interoperabile sia definita all'inizio del progetto in modo da essere applicata nei progetti relativi all'EES e all'ETIAS, dal momento che questi progetti forniscono e usano il BMS comune, l'archivio comune di dati di identità e il portale di ricerca europeo. Un membro del gruppo di gestione del progetto relativo all'interoperabilità dovrebbe far parte della struttura di governance del progetto dell'EES e dell'ETIAS.

2.2.3. Stima dei costi e dei benefici dei controlli e valutazione del previsto livello di rischio di errore

Non è fornita alcuna stima giacché il controllo e la riduzione dei rischi sono un compito intrinseco della struttura di governance del progetto.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste.

Le misure previste per combattere le frodi, previste all'articolo 35 del regolamento (UE) n. 1077/2011, sono le seguenti.

1. Ai fini della lotta contro la frode, la corruzione ed altri atti illeciti si applica il regolamento (CE) n. 1073/1999.

2. Le agenzie aderiscono all'accordo interistituzionale relativo alle indagini interne svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e adottano immediatamente le opportune disposizioni, applicabili a tutto il loro personale.

3. Le decisioni concernenti il finanziamento e i correlati accordi e strumenti di attuazione stabiliscono espressamente che la Corte dei conti e l'OLAF possono svolgere, se necessario, controlli in loco presso i beneficiari dei finanziamenti delle agenzie e gli agenti responsabili della loro assegnazione.

In conformità di tale disposizione il 28 giugno 2012 il consiglio di amministrazione dell'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia ha adottato la decisione relativa alle condizioni e alle modalità delle indagini interne in materia di lotta contro le frodi, la corruzione ed altri atti illeciti che ledono gli interessi dell'Unione.

Si applicherà la strategia della DG HOME in materia di prevenzione e individuazione delle frodi.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

LA STIMA DELL'INCIDENZA SULLA SPESA E SULL'ENTITÀ DEL PERSONALE NEGLI ANNI 2021 E OLTRE È INSERITA NELLA PRESENTE SCHEDA FINANZIARIA LEGISLATIVA A TITOLO PRETTAMENTE ILLUSTRATIVO E NON PREGIUDICA IL PROSSIMO QUADRO FINANZIARIO PLURIENNALE

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero [Denominazione……..……]	Diss./Non diss.[72].	di paesi EFTA[73]	di paesi candidati[74]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
3	18.02.01.03 – Frontiere intelligenti	Diss.	NO	NO	SÌ	NO
3	18.02.03 – Agenzia europea della guardia di frontiera e costiera (Frontex)	Diss.	NO	NO	SÌ	NO
3	18.02.04 – EUROPOL	Diss.	NO	NO	NO	NO
3	18.02.05 - CEPOL	Non diss.	NO	NO	NO	NO
3	18.02.07 – Agenzia europea per la gestione operativa di sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA)	Diss.	NO	NO	SÌ	NO

[72] Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.
[73] EFTA: Associazione europea di libero scambio.
[74] Paesi candidati e, se del caso, paesi potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

[Sezione da compilare utilizzando il **foglio elettronico sui dati di bilancio di natura amministrativa** (secondo documento allegato alla presente scheda finanziaria), da caricare su DECIDE a fini di consultazione interservizi.]

3.2.1. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	3	Sicurezza e cittadinanza

DG Home			Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**Anno 2028**	**TOTALE**
• Stanziamenti operativi													
18.02.01.03 – Frontiere intelligenti	Impegni	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Pagamenti	(2.	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici[75]													
Numero della linea di bilancio		(3)											
TOTALE degli stanziamenti per la DG Home	Impegni	=1+1a +3)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Pagamenti	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Le spese coprono i seguenti costi:

– I costi per adeguare la NUI (interfaccia uniforme nazionale) il cui sviluppo è finanziato nel quadro della proposta EES, un importo iscritto a bilancio per le modifiche dei sistemi degli Stati membri per tener conto delle modifiche dei sistemi centrali e un importo iscritto a bilancio per la formazione degli utenti finali.

[75] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

18.0203 – Guardia di frontiera e costiera europea			Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Titolo 1: Spese di personale	Impegni	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Pagamenti	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Titolo 2: Spese di infrastruttura e funzionamento	Impegni	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Pagamenti	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Titolo 3: Spese operative	Impegni	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Pagamenti	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
TOTALE degli stanziamenti per Europol	(Totale impegni = Totale pagamenti)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– Il bilancio per la guardia di frontiera e costiera europea copre le spese di un gruppo incaricato della convalida dei collegamenti generati dal MID (rivelatore di identità multiple) sull'insieme di dati (circa 14 milioni di registrazioni). Si stima che i collegamenti da convalidare manualmente siano circa 550 000.
  L'apposito gruppo istituito a tal fine si aggiunge al gruppo della guardia di frontiera e costiera europea istituito per l'ETIAS poiché è funzionalmente vicino e si evitano i costi di creazione di un nuovo gruppo. I lavori dovrebbero essere effettuati nel 2023. Gli agenti contrattuali saranno quindi assunti fino a 3 mesi prima, e il loro contratto terminerà fino a 2 mesi dopo la conclusione dell'attività di migrazione. Un'altra parte delle risorse necessarie dovrebbe essere assunta non come agente contrattuale bensì come consulente. Questo spiega le spese del titolo 3 per il 2023. Si presume che questo personale sia assunto un mese prima. Ulteriori dettagli sull'organico sono forniti in seguito.

– Il titolo 1 comprende pertanto il costo di 20 membri del personale interno, e le disposizioni per il rafforzamento del personale di gestione e di sostegno.

– Il titolo 2 comprende il costo aggiuntivo per ospitare i 10 membri aggiuntivi del personale del contraente.

– Il titolo 3 comprende le spese per i 10 membri aggiuntivi del personale del contraente. Non sono inclusi altri tipi di costi.

18.0204 - Europol			Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Titolo 1: Spese di personale	Impegni	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Pagamenti	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Titolo 2: Spese di infrastruttura e funzionamento	Impegni	(1a)	0	0	0	0	0	0	0	0	0	0
	Pagamenti	(2a)	0	0	0	0	0	0	0	0	0	0
Titolo 3: Spese operative	Impegni	(3a)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
	Pagamenti	(3b)	0	6,380	6,380	2,408	2,408	7,758	7,758	7,758	2,408	37,908
TOTALE degli stanziamenti per Europol	(Totale impegni = Totale pagamenti)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Le spese di Europol copriranno l'aggiornamento delle capacità dei sistemi TIC di Europol per far fronte al volume di messaggi da gestire, e il necessario aumento dei livelli di prestazione (tempi di risposta).

Titolo 1: le spese di personale comprendono le spese per l'assunzione di personale TIC supplementare per rafforzare i sistemi d'informazione di Europol per i motivi descritti sopra. Ulteriori dettagli sulla ripartizione dei posti tra agenti temporanei e agenti contrattuali e sulle loro competenze sono fornite sotto.

Il titolo 3 comprende i costi di hardware e software necessari per rafforzare i sistemi d'informazione di Europol. Attualmente, i sistemi informatici di Europol servono una limitata comunità designata di Europol, ufficiali di collegamento Europol e investigatori degli Stati membri che utilizzano tali sistemi a fini di analisi e di indagine. Con l'attuazione di QUEST (l'interfaccia di sistema che consentirà all'ESP di interrogare i dati Europol) a un livello di protezione minimo (attualmente i sistemi d'informazione di Europol sono accreditati fino al livello RESTREINT UE/EU RESTRICTED e UE riservati), i sistemi di informazione Europol saranno messi a disposizione di una comunità autorizzata delle autorità di contrasto molto più ampia. Oltre a tali aumenti, l'ESP sarà usato dall'ETIAS per interrogare automaticamente i dati Europol per trattare le autorizzazioni ai viaggi. Ne conseguirà un aumento del volume delle interrogazioni dei dati Europol, passando dalle attuali circa 107 000 interrogazioni al mese a più di 100 000 interrogazioni al giorno, e occorrerà che i sistemi di informazione Europol siano disponibili 24/7 e che i tempi di risposta siano molto brevi per soddisfare i requisiti imposti dal regolamento ETIAS. La maggior parte delle spese sono limitate al periodo precedente l'entrata in funzione delle componenti dell'interoperabilità, ma sono necessari alcuni impegni correnti per garantire una

disponibilità elevata e costante dei sistemi di informazione Europol. Inoltre, occorrono alcuni lavori di sviluppo per attuare le componenti dell'interoperabilità da parte di Europol come utente.

18.0205 - CEPOL			Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Titolo 1: Spese di personale	Impegni	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Pagamenti	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Titolo 2: Spese di infrastruttura e funzionamento	Impegni	(1a)	0	0	0	0	0	0	0	0	0	0
	Pagamenti	(2a)	0	0	0	0	0	0	0	0	0	0
Titolo 3: Spese operative	Impegni	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Pagamenti	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
TOTALE degli stanziamenti per CEPOL	(Totale impegni = Totale pagamenti)	=1+1a +3a	0	0,144	0.384,	0,482	0,208	0,208	0,208	0,208	0,208	2,050

La formazione coordinata a livello centrale dell'UE migliora l'attuazione coerente dei corsi di formazione a livello nazionale e, di conseguenza, garantisce l'attuazione e l'uso corretti ed efficaci delle componenti dell'interoperabilità. CEPOL, l'Agenzia dell'UE per la formazione delle autorità di contrasto, è ben posizionata per fornire formazione a livello centrale dell'UE. Queste spese coprono la preparazione della "formazione dei formatori degli Stati membri" necessaria per usare i sistemi centrali una volta resi interoperabili. Le spese includono le spese legate ad un leggero aumento del personale di CEPOL per coordinare, gestire, organizzare e aggiornare i corsi e il costo per la fornitura di una serie di sessioni di formazione all'anno e la preparazione del corso online. I dettagli di questi costi sono illustrati sotto. Gli sforzi di formazione si concentrano nei periodi immediatamente precedenti l'entrata in funzione. Sulla base dell'esperienza di formazione in materia di sistema d'informazione Schengen, è necessario uno sforzo continuo al di là dell'entrata in funzione giacché le componenti dell'interoperabilità sono mantenute e i formatori non rimangono sempre gli stessi.

18.0207 - eu-LISA			Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Titolo 1: Spese di personale	Impegni	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Pagamenti	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Titolo 2: Spese di infrastruttura e funzionamento	Impegni	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Pagamenti	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Titolo 3: Spese operative	Impegni	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Pagamenti	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
TOTALE degli stanziamenti per eu-LISA	(Totale impegni = Totale pagamenti)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Queste spese copriranno:

– Lo sviluppo e la manutenzione delle quattro componenti dell'interoperabilità - portale di ricerca europeo (ESP), servizio comune di confronto biometrico (BMS comune), archivio comune di dati di identità (CIR) e rilevatore di identità multiple (MID) - di cui alla proposta legislativa nonché dell'archivio centrale di relazioni e statistiche (CRRS). eu-LISA sarà il rappresentante del titolare del progetto e userà il proprio personale per la redazione dei capitolati d'oneri, la selezione dei contraenti, la direzione dei lavori, la sottoposizione dei risultati a una serie di test e l'accettazione dei lavori svolti.

– I costi connessi con la migrazione dei dati dei sistemi preesistenti verso le nuove componenti. eu-LISA non ha tuttavia un ruolo diretto nel caricamento iniziale dei dati per il MID (la convalida dei collegamenti) perché si tratta di un'azione sul contenuto stesso dei dati. La migrazione dei dati biometrici dei sistemi preesistenti riguarda il formato e l'etichetta dei dati, e non il contenuto dei dati.

– I costi per aggiornare e far funzionare l'ECRIS-TCN come sistema ad alta disponibilità a partire dal 2022. L'ECRIS-TCN è il sistema centrale che contiene i casellari giudiziali dei cittadini di paesi terzi. Il sistema dovrebbe essere reso disponibile entro il 2020. Anche le componenti dell'interoperabilità dovrebbero accedere a tale sistema, che pertanto dovrebbe diventare un sistema ad alta disponibilità. Le spese operative comprendono il costo supplementare per conseguire tale elevato livello di disponibilità. Vi è un notevole costo di sviluppo nel 2021, seguito

da costi correnti di manutenzione e funzionamento. Tali costi non sono inclusi nella scheda finanziaria legislativa relativa alla revisione del regolamento istitutivo di eu-LISA[76], che include esclusivamente i bilanci dal 2018 al 2020 e pertanto non si sovrappone a questa richiesta di bilancio.

– Il ritmo delle spese è il risultato della programmazione del progetto. Poiché le diverse componenti non sono indipendenti le une dalle altre, il periodo di sviluppo si estende dal 2019 al 2023. Tuttavia a partire dal 2020 iniziano già la manutenzione il funzionamento delle prime componenti disponibili. Ciò spiega perché le spese di avvio iniziano lentamente, aumentano e poi diminuiscono a un valore costante.

– Le spese del titolo 1 (spese di personale) seguono la programmazione del progetto: un maggior numero di personale è tenuto a realizzare il progetto con il contraente (le cui spese rientrano nel titolo 3). Una volta realizzato il progetto, parte del gruppo che era preposto alla realizzazione del progetto è incaricato dell'evoluzione e della manutenzione. Parallelamente aumenta il personale per la gestione dei nuovi sistemi.

– Le spese del titolo 2 (spese di infrastruttura e funzionamento) coprono l'ulteriore spazio per gli uffici necessario per ospitare temporaneamente il gruppo del personale del contraente preposto allo sviluppo, alla manutenzione e al funzionamento. Il ritmo delle spese pertanto segue anche l'evoluzione del personale. Le spese per ospitare attrezzature supplementari sono già state incluse nel bilancio di eu-LISA. Non vi sono spese aggiuntive per ospitare il personale di eu-LISA, in quanto sono già incluse nelle spese di personale.

– Le spese del titolo 3 (spese operative) comprendono le spese del contraente per lo sviluppo e la manutenzione del sistema e l'acquisizione di hardware e software specifici.
  Le spese del contraente cominciano con gli studi per specificare le componenti, e lo sviluppo inizia solo per una componente (il CRRS). Nel periodo 2020-2022 le spese aumentano giacché più componenti sono sviluppate in parallelo. Le spese non diminuiscono dopo il picco poiché i compiti relativi alla migrazione dei dati sono particolarmente impegnativi in questo portafoglio di progetti. Le spese del contraente poi calano una volta che le componenti sono state realizzate ed entrano in funzione, il che richiede una struttura stabile di risorse.
  Contestualmente alle spese del titolo 3, nel 2020 la spesa aumenta notevolmente rispetto all'anno precedente a causa dell'investimento iniziale per l'hardware e il software necessari durante lo sviluppo. Le spese del titolo 3 (spese operative) subiscono un'impennata nel 2021 e nel 2022 a causa dei costi di investimento in hardware e software per gli ambienti informatici operativi (produzione e pre-produzione sia per l'unità centrale che per l'unità centrale di riserva) sostenuti l'anno precedente all'entrata in funzione, rispettivamente per le componenti dell'interoperabilità (CIR e MID) con elevati requisiti in materia di software e hardware. Una volta in funzione, le spese per l'hardware e il software rientrano essenzialmente tra le spese di manutenzione.

– Informazioni più dettagliate sono fornite sotto.

[76] COM 2017/0145 (COD) Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, che modifica il regolamento (CE) n. 1987/2006 e la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (UE) n. 1077/2011

Rubrica del quadro finanziario pluriennale	**5**	"Spese amministrative"

Mio EUR (al terzo decimale)

		Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
DG HOME											
•Risorse umane Numero della linea di bilancio 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Altre spese amministrative (riunioni, ecc.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
TOTALE DG HOME	Stanziamenti	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

Mio EUR (al terzo decimale)

		Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	Anno **2028**	**TOTALE**
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Pagamenti	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**

3.2.2. Incidenza prevista sugli stanziamenti operativi

3.2.2.1. Incidenza prevista sugli stanziamenti dell'Agenzia europea della guardia di frontiera e costiera

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
Agenzia europea della guardia di frontiera e costiera ⇩	Tipo[77]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[78] Convalida dei collegamenti																						
N. di personale assunto in qualità di esperti per convalidare i collegamenti	Spese del contraente		0	0	0	0	0	0	0.8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Totale parziale dell'obiettivo specifico 1			**0**	**0**	**0**	**0**	**0**	**0**	**0.8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

[77] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

[78] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

Queste spese copriranno:

- L’assunzione di personale supplementare sufficiente (circa 10 esperti) per il personale interno esistente (circa 20 persone) che sarà ospitato presso la guardia di frontiera e costiera europea per convalidare i collegamenti. Vi è solo un mese per procedere alle assunzioni prima della data di inizio pianificata per raggiungere i necessari livelli di personale.

- Non vi sono altre spese stimate per il contraente. Il software necessario fa parte delle spese di licenza del BMS comune. Non c’è una specifica capacità di trattamento dell’hardware. Si presume che il personale del contraente sarà ospitato presso la guardia di frontiera e costiera europea. Pertanto nelle spese del titolo 2 è aggiunta la spesa annua di 12 metri quadri in media per persona.

3.2.2.2. Incidenza prevista sugli stanziamenti di Europol

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
Europol ⇩	Tipo[79]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[80] Sviluppo e manutenzione dei sistemi (di Europol)																						
Ambiente IT	Infrastruttura					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
Ambiente IT	Hardware					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144
Ambiente IT	Software					0,670		0,670		0,268		0,268		0,268		0,268		0,268		0,268		2,948
Lavori di sviluppo	Contraente					0,360		0,360														0,720
Totale parziale				**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

[79] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

[80] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

Tali spese copriranno la necessità di potenziare i sistemi d'informazione di Europol e le sue infrastrutture per far fronte all'aumento delle interrogazioni. Tali spese comprendono:

- miglioramento della sicurezza e dell'infrastruttura di rete, dell'hardware (server, archiviazione) e del software (licenze). Questi miglioramenti devono essere ultimati prima che il portale di ricerca europeo e l'ETIAS entrino in funzione nel 2021; le spese sono state equamente ripartite tra il 2020 e il 2021. A partire dal 2022 è stato preso come base di calcolo delle spese un tasso di manutenzione annuale del 20%. Inoltre, è stato preso in considerazione il normale ciclo di cinque anni per la sostituzione di hardware e infrastrutture obsoleti.
- le spese di sviluppo del contraente per attuare QUEST al livello di protezione minimo.

3.2.2.3. Incidenza prevista sugli stanziamenti di CEPOL

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
CEPOL ⇩	Tipo[81]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[82] Sviluppo e realizzazione dei corsi di formazione																						
Numero di corsi residenziali	0,34 per corso		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Formazione online	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Totale parziale				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

[81] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

[82] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

Per garantire l'attuazione e l'uso uniformi delle soluzioni dell'interoperabilità, la formazione sarà organizzata sia centralmente a livello dell'UE da CEPOL sia dagli Stati membri. La spesa per la formazione a livello dell'UE comprende:

- lo sviluppo di programmi di formazione comune destinati ad essere usati dagli Stati membri nell'attuazione della formazione nazionale;

- le attività residenziali per la formazione dei formatori. Nei due anni immediatamente successivi all'entrata in funzione delle soluzioni dell'interoperabilità la formazione dovrebbe essere attuata su scala più ampia e poi essere mantenuta tramite due corsi di formazione residenziale all'anno;

- corso online per integrare le attività residenziali a livello dell'UE e negli Stati membri.

3.2.2.4. Incidenza prevista sugli stanziamenti di eu-LISA

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati **eu-LISA** ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo[83]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[84] Sviluppo delle componenti dell'interoperabilità																						
Sistemi realizzati	Contraente			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Prodotti software	Software			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Prodotti hardware	Hardware			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
Formazione IT	Formazione e altro			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340
Totale parziale dell'obiettivo specifico 1				**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

[83] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

[84] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

– Questo obiettivo comprende solo le spese per la realizzazione delle quattro componenti dell'interoperabilità e del CRRS.

– Le spese per il BMS comune sono state stimate partendo dal presupposto che l'EES che sta per essere sviluppato fungerà da sistema di base per lo sviluppo. Pertanto, si prevede di sfruttare le licenze del software biometrico (36 milioni di EUR) previste per l'EES.

– In questo bilancio, il BMS comune è trattato in termini di bilancio come un'ulteriore estensione del BMS per l'EES. Pertanto l'attuale scheda finanziaria comprende il costo marginale per le licenze di software (6,8 milioni di EUR) per aggiungere i circa 20 milioni di insiemi di dati biometrici contenuti nell'AFIS del SIS (l'AFIS è il sistema automatizzato di identificazione delle impronte digitali, vale a dire il "BMS" del SIS), nell'AFIS dell'Eurodac e nel futuro sistema ECRIS-TCN (il sistema europeo di informazione sui casellari giudiziali per i cittadini di paesi terzi) al BMS realizzato per l'EES. Il costo dell'integrazione dei diversi sistemi (SIS, Eurodac, ECRIS) nel BMS comune sono inclusi in questa scheda finanziaria.

– Come parte dei lavori del 2019 e del 2020, eu-LISA sarà invitata a progettare la precisa soluzione tecnica che non può essere definita al momento della presentazione della proposta legislativa e a stimare le conseguenze in termini di costi per l'attuazione della soluzione tecnica prescelta. Ciò può comportare un cambiamento della stima dei costi fornita in questa sede.

– Tutte le componenti sono realizzate entro la fine del 2023, il che spiega perché le spese del contraente si riducono quasi a zero entro tale termine. Rimane solo un importo residuo per l'aggiornamento periodico del CRSS.

– Nel periodo tra il 2019 e il 2021 le spese di software aumentano considerevolmente a causa delle spese per le licenze software sostenute per i differenti ambienti necessari per la produzione, la preproduzione e la sperimentazione tanto sul sito centrale quanto su quello di riserva. Inoltre, alcuni componenti di software specifici e indispensabili hanno un prezzo basato sul numero di "oggetti di riferimento" (ossia il volume di dati). Poiché la banca dati conterrà circa 220 milioni di identità, il prezzo del software è proporzionato a tale valore.

Specificare gli obiettivi e i risultati eu-LISA ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo[85]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 2 Manutenzione e funzionamento delle componenti dell'interoperabilità																						
Sistemi mantenuti in funzione	Contraente			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Prodotti software	Software			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Prodotti hardware	Hardware			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
Formazione IT	Formazione			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Totale parziale dell'obiettivo specifico 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– La manutenzione ha inizio non appena le componenti sono realizzate. Pertanto il bilancio per un contraente preposto alla manutenzione è incluso dal momento in cui l'ESP è realizzato (nel 2021). Il bilancio per la manutenzione aumenta man mano che le varie componenti sono realizzate e poi raggiunge un valore più o meno costante che rappresenta una percentuale (compresa tra il 15 e il 22%) dell'investimento iniziale.

[85] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

– La manutenzione per l'hardware e il software inizia dall'anno di entrata in funzione: l'evoluzione delle spese è simile a quella delle spese del contraente.

Specificare gli obiettivi e i risultati **eu-LISA** ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo[86]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 3[87] Dati migrati																						
Dati BMS migrati	Verso il BMS comune			0		0		0		7,000		3,000		0		0		0		0		10,000
Dati EDAC idonei alla migrazione	Riprogettazione e riorganizzazione dell'EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Totale parziale dell'obiettivo specifico 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– Nel caso del progetto relativo al BMS comune, i dati devono essere fatti migrare dagli altri dispositivi biometrici verso il BMS comune poiché questo sistema comune è più efficace dal punto di vista operativo e fornisce anche un vantaggio finanziario rispetto alla situazione in cui continuano ad essere mantenuti vari sistemi BMS di dimensioni inferiori.

– L'attuale logica di funzionamento di Eurodac non è chiaramente separata dal meccanismo di confronto biometrico, come invece è il caso per il BMS che opera con il VIS. Il funzionamento interno di Eurodac e il meccanismo con cui i servizi operativi chiamano i sottostanti servizi di confronto biometrico sono una scatola nera visti dall'esterno e si basano su tecnologie proprietarie. Non sarà possibile limitarsi a migrare i dati

[86] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).
[87] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

in un BMS comune e mantenere l'attuale livello operativo. Pertanto la migrazione dei dati è accompagnata da spese considerevoli per la modifica dei meccanismi di scambio con l'applicazione centrale di Eurodac.

Specificare gli obiettivi e i risultati **eu-LISA** ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo[88]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 4[89] Rete																						
Connessioni alla rete	Creazione della rete			0		0		0		0,505										0		0,505
Traffico di rete gestito	Funzionamento della rete			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Totale parziale dell'obiettivo specifico 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– Le componenti dell'interoperabilità hanno solo un effetto marginale sul traffico di rete. In termini di dati, sono creati solo i collegamenti tra i dati già esistenti, il che è un elemento di volume modesto. I costi inclusi qui sono solo l'aumento marginale del bilancio necessario in aggiunta ai bilanci dell'EES e dell'ETIAS per la creazione della reta e il traffico di rete.

[88] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).
[89] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

Specificare gli obiettivi e i risultati eu-LISA ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo[90]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 5[91] Aggiornamento NUI																						
NUI aggiornate	Contraente			0		0		0		0,505		0,505								0		1,010
Totale parziale dell'obiettivo specifico 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– La proposta relativa all'EES ha introdotto il concetto di interfaccia uniforme nazionale (NUI) che dovrà essere sviluppata e mantenuta da eu-LISA. La tabella qui sopra presenta il bilancio per l'aggiornamento della NUI per un ulteriore tipo di scambio di informazioni. Non ci sono costi aggiuntivi per il funzionamento della NUI, che erano già stati iscritti a bilancio nel quadro della proposta EES.

[90] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).
[91] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

Specificare gli obiettivi e i risultati eu-LISA ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo [92]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 6 Riunioni e formazione																						
Riunioni mensili sullo stato di avanzamento (Sviluppo)		0,021 per riunione x 10 all'anno	10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Riunioni trimestrali (funziona-mento)		0,021 x 4 all'anno	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Gruppi consultivi		0,021 x 4 all'anno	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Formazione Stati membri		0,025 per formazione	2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Totale parziale dell'obiettivo specifico 6			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

[92] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

– Il totale parziale 6 comprende i costi di organizzazione di riunioni da parte dell'autorità di gestione (in questo caso eu-LISA) per la governance del progetto. Si tratta delle spese per riunioni supplementari per la realizzazione delle componenti dell'interoperabilità.

– Il totale parziale 6 comprende le spese per le riunioni di eu-LISA con il personale degli Stati membri che si occupa dello sviluppo, della manutenzione e del funzionamento delle componenti dell'interoperabilità e dell'organizzazione e fornitura della formazione per il personale informatico degli Stati membri.

– Durante lo sviluppo, il bilancio comprende 10 riunioni di progetto all'anno. Una volta che si preparerà il funzionamento (ossia dal 2019 in poi) saranno organizzate quattro riunioni all'anno. Ad un livello più alto, fin dall'inizio è istituito un gruppo consultivo per attuare le decisioni di esecuzione della Commissione. Sono previste quattro riunioni all'anno, come per gli attuali gruppi consultivi. Inoltre, eu-LISA elabora e fornisce formazioni per il personale informatico degli Stati membri. Si tratta di una formazione sugli aspetti tecnici delle componenti dell'interoperabilità.

Specificare gli obiettivi e i risultati **eu-LISA** ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo[93]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 7[94] Alta disponibilità dell'ECRIS-TCN																						
Sistema ad alta disponibilità	Creazione del sistema			0		0		8,067												0		8,067

[93] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

[94] Come descritto nella sezione 1.4.2. "Obiettivi specifici e attività ABM/ABB interessate".

Funzionamento ad alta disponibilità,	Sistema sottoposto a manutenzione e tenuto in funzione		0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Totale parziale dell'obiettivo specifico 4			**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– L'obiettivo 7 è di trasformare ECRIS-TCN da sistema a disponibilità "standard" a sistema ad alta disponibilità. Nel 2021 ECRIS-TCN verrà sottoposto a tale miglioramento, che richiede essenzialmente l'acquisizione di hardware supplementare. Poiché il sistema ECRIS-TCN dovrebbe essere ultimato nel 2020, si potrebbe ipotizzare di renderlo ad alta disponibilità fin dall'inizio e integrarlo alle componenti dell'interoperabilità. Tuttavia, dato che molti progetti dipendono l'uno dall'altro, è prudente non partire da questo assunto e imputare a bilancio azioni distinte. Questo bilancio si aggiunge alle spese di sviluppo, manutenzione o funzionamento dell'ECRIS-TCN nel 2019 e nel 2020.

3.2.2.5. Incidenza prevista sugli stanziamenti della DG Home

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati **DG Home** ⇩			Anno **2019**		Anno **2020**		Anno **2021**		Anno **2022**		Anno **2023**		Anno **2024**		Anno **2025**		Anno **2026**		Anno **2027**		**TOTALE**	
	Tipo [95]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1 Integrazione dei sistemi nazionali (degli Stati membri)																						
NUI pronte all'uso	Personalizzazione della NUI - sviluppi						30	3,150	30	3,150											30	6,300
Sistemi degli Stati membri adattatati all'interoperabilità	Costi di integrazione						30	40,000	30	40,000	30	40,000									30	120,000

[95] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

Utenti finali formati	10 000 sessioni per gli utenti finali al costo di 1 000 EUR per sessione							5000	5,000	5000	5,000								10.000	10,000
Totale parziale dell'obiettivo specifico 1							**43,150**		**48,150**		**45,000**									**136,300**

– L'obiettivo specifico 1 riguarda i fondi messi a disposizione degli Stati membri affinché traggano vantaggio dai sistemi centrali interoperabili. La NUI è personalizzata sia quando è attuato l'ESP sia quando il MID diventa operativo. Ciascuno Stato membro deve quindi effettuare cambiamenti relativamente modesti (stimati a 150 giorni/uomo) per adattarsi a questi scambi di messaggi aggiornati con i sistemi centrali. Più rilevante è invece la modifica del contenuto dei dati che sarà introdotta dall'interoperabilità e che rientra nella categoria "spese di integrazione". Tali fondi riguardano le modifiche dei messaggi trasmessi al sistema centrale e per il trattamento delle risposte. Per stimare i costi di tali modifiche, è assegnata una dotazione di 4 milioni di EUR a ciascuno Stato membro. Tale importo è lo stesso previsto per l'EES, in quanto il volume di lavoro necessario per adattare l'integrazione dei sistemi nazionali con la NUI è comparabile.

– Gli utenti finali devono essere formati ai sistemi. Tale formazione, destinata a una popolazione molto ampia di utenti finali, deve essere finanziata sulla base di 1 000 EUR per sessione, ciascuna con un numero di utenti finali che va da 10 a 20 persone, per 10 000 sessioni stimate che dovranno essere organizzate da tutti gli Stati membri nei loro locali.

3.2.3. Incidenza prevista sulle risorse umane

3.2.3.1. Agenzia europea della guardia di frontiera e costiera - Sintesi

☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Funzionari (gradi AD)										
Funzionari (gradi AST)	0									
Agenti contrattuali	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Agenti temporanei	0	0	0	0	0	0	0	0	0	0
Esperti nazionali distaccati										

TOTALE	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	0,233	0,0	**0,0**	**0,0**	**1,983**

Il lavoro previsto del personale supplementare della guardia di frontiera e costiera europea è limitato nel tempo (2023, ossia 24 mesi dopo la data di disponibilità del dispositivo biometrico per l'EES). Tuttavia il personale deve essere assunto in anticipo (è calcolata una media di tre mesi), il che spiega il valore per il 2022. Una volta effettuato il lavoro, dovranno essere svolti alcuni compiti conclusivi/finali che dureranno due mesi, il che spiega il livello di organico nel 2024.

Il livello di organico in sé si basa su 20 persone necessarie per il lavoro da svolgere (più 10 persone fornite da un contraente, di cui si tiene conto nel titolo 3). Si prevede che i compiti siano svolti anche al di fuori dell'orario di lavoro standard. Si parte dal presupposto che il personale di supporto e direttivo sia fornito sulla base delle risorse dell'Agenzia.

Il numero degli effettivi è basato sull'ipotesi che dovranno essere valutate circa 550 000 impronte digitali in un tempo medio di 5-10 minuti per caso (17 000 impronte all'anno verificate)[96].

[96] L'organico nel 2020 e negli anni successivi è indicativo; bisognerà valutare se debba andare ad aggiungersi o meno alle previsioni di personale della guardia di frontiera e costiera europea di cui al COM(2015) 671.

Numero di personale	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Personale per trattare manualmente i collegamenti e le decisioni	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Totale Titolo 1 - AC	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Totale Titolo 1 - AT	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Totale Titolo 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

3.2.3.2. Europol - Sintesi

☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Funzionari (gradi AD)										
Funzionari (gradi AST)	0									
Agenti contrattuali	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Agenti temporanei	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Esperti nazionali distaccati										
TOTALE	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Questi costi sono stimati sulla base dei seguenti livelli di organico:

Numero di ETP per le TIC	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totale**
Agenti contrattuali	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Agenti temporanei	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Totale effettivi (ETP)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

È previsto personale TIC supplementare per Europol per rafforzarne i sistemi d'informazione al fine di far fronte all'aumento del numero di interrogazioni dall'ESP e dall'ETIAS e, successivamente, per mantenere i sistemi 24/7.

– Per la fase di attuazione dell'ESP (2020 e 2021), vi è un'ulteriore esigenza di esperti tecnici (architetti, ingegneri, sviluppatori, collaudatori). Dal 2022 in poi occorrerà un numero ridotto di esperti tecnici per attuare le restanti componenti dell'interoperabilità e mantenere i sistemi.

– A partire dal secondo semestre del 2021 deve essere attuato un monitoraggio del sistema TIC 24/7 per garantire i livelli di servizio dell'ESP e dell'ETIAS. Questo compito sarà effettuato da 2 agenti contrattuali, che lavoreranno in 4 turni 24/7.

– Nella misura del possibile, i profili sono stati suddivisi tra agenti temporanei e agenti contrattuali. Va notato tuttavia che a causa degli elevati requisiti di sicurezza, per alcuni posti è possibile ricorrere solo ad agenti temporanei. La richiesta di agenti temporanei terrà conto dei risultati della concertazione della procedura di bilancio per il 2018.

3.2.3.3. CEPOL - Sintesi

☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Funzionari (gradi AD)										
Funzionari (gradi AST)										
Agenti contrattuali			0,070	0,070						**0,140**
Agenti temporanei		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Esperti nazionali distaccati										
TOTALE		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

È necessario personale supplementare per sviluppare la formazione per i formatori degli Stati membri in vista dell'uso delle componenti dell'interoperabilità in condizioni operative.

- Lo sviluppo dei programmi di studio e dei moduli di formazione dovrebbe iniziare almeno 8 mesi prima che il sistema entri in funzione. Nei primi due anni dopo l'entrata in funzione la

formazione sarà più intensa e dovrà proseguire per un periodo più lungo per garantire un'attuazione coerente, sulla base dell'esperienza acquisita con il sistema d'informazione Schengen.

- Il personale supplementare è necessario per preparare, coordinare e attuare il piano di studi, i corsi residenziali e il corso online. Questi corsi possono essere attuati solo in aggiunta alle attuali offerte di formazione di CEPOL, pertanto è necessario personale supplementare.

- Per tutto il periodo di sviluppo e manutenzione è previsto un gestore dei corsi, assunto come agente temporaneo, che sarà affiancato da un agente contrattuale nel periodo più intenso di organizzazione della formazione.

3.2.3.4. Eu-LISA - Sintesi

☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
Funzionari (gradi AD)										
Funzionari (gradi AST)										
Agenti contrattuali	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570
Agenti temporanei	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Esperti nazionali distaccati										
TOTALE	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– Il fabbisogno di personale tiene conto del fatto che le quattro componenti e il CRRS costituiscono un portafoglio di progetti con interdipendenze (ossia un programma). Per gestire i legami di dipendenza tra i progetti, è creato un gruppo di gestione del programma, che comprende i responsabili del programma e dei progetti e i profili (spesso indicati come architetti) che devono definire gli elementi comuni. La realizzazione del programma/dei progetti richiede altresì profili per il sostegno al programma e ai progetti.

– Il fabbisogno di personale per progetto è stato stimato per analogia con i progetti precedenti (sistema di informazione visti) e distinguendo tra la fase di completamento del progetto e la fase operativa.

– I profili che devono rimanere durante la fase operativa sono assunti come agenti temporanei. I profili richiesti durante l'esecuzione del programma/dei progetti sono assunti come agenti contrattuali. Al fine di garantire la continuità dei compiti e mantenere le conoscenze in seno all'Agenzia, il numero di posti è ripartito circa 50/50 tra agenti temporanei e agenti contrattuali.

– Si presuppone che non sarà necessario personale supplementare per il progetto di alta disponibilità dell'ECRIS-TCN e che per il progetto relativo a eu-LISA sarà riutilizzato il personale esistente liberatosi da progetti che giungono a completamento in quel periodo.

Queste stime sono basate sui seguenti livelli di organico:

Per gli agenti contrattuali:

3.2.1. risultati EU-LISA (è uguale a T1) in numero di persone	2019	2020	2021	2022	2023	2024	2025	2026	2027	Totale (formula)
Agenti contrattuali										-
Gestione del programma/progetto	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
CRRS PM	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Ufficio del programma/progetto	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Garanzia della qualità	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Aspetti finanziari e appalti	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gestione finanziaria										*0,0*
Pianificazione di bilancio e controllo										*0,0*
Gestione dell'appalto/del contratto	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Esperti tecnici	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
BMS comune	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Collaudo	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS comune	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Monitoraggio del sistema	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Comune (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Coordinamento generale	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Risorse umane	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Totale parziale agenti contrattuali	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

Per gli agenti temporanei:

Agenti temporanei										
Gestione del programma/progetto	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Gestione del programma	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestione del programma/progetto	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Ufficio del programma/progetto	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
BMS comune	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Aspetti finanziari e appalti	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Gestione finanziaria	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Pianificazione di bilancio e controllo	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestione dell'appalto/del contratto	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Esperti tecnici	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS comune	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Sicurezza	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architetti	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Collaudo	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
BMS comune	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Monitoraggio del sistema	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS comune	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Formazione	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Formazione	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Risorse umane	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
HR	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Altro	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Specialista protezione dati	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Totale parziale agenti temporanei	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Totale	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.4.1. DG Home: Sintesi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
RUBRICA 5 del quadro finanziario pluriennale										
Risorse umane DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Altre spese amministrative	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Totale parziale della RUBRICA 5 del quadro finanziario pluriennale	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Esclusa la RUBRICA 5[97] del quadro finanziario pluriennale	(non utilizzato)									
Risorse umane										
Altre spese di natura amministrativa										
Totale parziale esclusa la RUBRICA 5 del quadro finanziario pluriennale										

TOTALE	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

[97] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.4.2. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ☒ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

	Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
• Posti della tabella dell'organico (funzionari e agenti temporanei)										
18 01 01 01 (in sede e negli uffici di rappresentanza della Commissione) DG HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (nelle delegazioni)										
XX 01 05 01 (ricerca indiretta)										
10 01 05 01 (ricerca diretta)										
• Personale esterno (in equivalenti a tempo pieno: ETP)[98]										
XX 01 02 02 (AC, AL, END, INT e JED nelle delegazioni)										
XX 01 04 **yy**[99] - in sede										
XX 01 04 **yy**[99] - nelle delegazioni										
XX 01 05 02 (AC, END e INT – ricerca indiretta)										
10 01 05 02 (AC, END e INT – ricerca diretta)										
Altre linee di bilancio (specificare)										
TOTALE	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Monitoraggio del progetto e follow-up. Tre funzionari per il follow-up. Il personale si occupa dei compiti della Commissione in relazione alla realizzazione del programma: verificare la conformità con la proposta legislativa, trattare le questioni di conformità, preparare le relazioni da presentare al Parlamento europeo e al Consiglio, valutare i progressi compiuti dagli Stati membri. Poiché il programma costituisce un'attività aggiuntiva rispetto al carico di lavoro attuale, occorre personale supplementare. Questo aumento dell'organico è limitato nel tempo e copre solo il periodo di sviluppo.

Gestione dello standard UMF

La Commissione gestirà lo standard UMF su base giornaliera. A tal fine sono necessari due funzionari: una persona in qualità di esperto in materia di attività di contrasto e un'altra persona con una buona conoscenza della modellazione operativa e con una conoscenza delle TIC.

Lo standard del formato universale dei messaggi (UMF) definisce le norme per uno scambio di informazioni transfrontaliero strutturato tra i sistemi di informazione, le autorità e/o le organizzazioni del settore Giustizia e

[98] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JED = giovane esperto in delegazione (jeune expert en délégation).

[99] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

affari interni. Lo standard UMF definisce un vocabolario comune e strutture logiche per le informazioni comunemente scambiate al fine di facilitare l'interoperabilità, consentendo la creazione e la lettura di contenuti dello scambio in modo coerente e semanticamente equivalente.

Al fine di garantire condizioni uniformi per l'attuazione del formato universale dei messaggi, è proposto che siano conferite alla Commissione competenze di esecuzione. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione.

3.2.5. Compatibilità con il quadro finanziario pluriennale attuale

– ☐ La proposta/iniziativa è compatibile con il quadro finanziario pluriennale attuale.

– ☒ La proposta/iniziativa richiede una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

Spiegare la riprogrammazione richiesta, precisando le linee di bilancio interessate e gli importi corrispondenti.

Il regolamento ISF-Frontiere è lo strumento finanziario in cui è stato inserito il bilancio per l'attuazione dell'iniziativa sull'interoperabilità.

Esso prevede, all'articolo 5, paragrafo 5, lettera b), che 791 milioni di EUR siano attuati tramite un programma per lo sviluppo di sistemi informatici basati su sistemi esistenti e/o nuovi a sostegno della gestione dei flussi migratori attraverso le frontiere esterne previa adozione dei pertinenti atti legislativi dell'Unione e nel rispetto delle condizioni di cui all'articolo 15, paragrafo 5. Di questi 791 milioni di EUR, 480,2 milioni sono riservati allo sviluppo dell'EES, 210 milioni per l'ETIAS e 67,9 milioni per la revisione del SIS II. Quel che resta (32,9 milioni di EUR) va riattribuito secondo i meccanismi dell'ISF-Frontiere. **Per il rimanente periodo coperto dal quadro finanziario pluriennale attuale, la presente proposta necessita di una dotazione pari a 32,1 milioni di EUR, vale a dire un importo rientrante nella dotazione restante**.

La conclusione di cui al precedente riquadro riguardo all'importo necessario di 32,1 milioni di EUR è il risultato del seguente foglio di calcolo:

IMPEGNI										
3.2. Incidenza prevista sulle spese DG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (horiz)**
18 02 01 03 - Frontiere intelligenti (copre il sostegno agli SM)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Totale (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formula)**
T1: Spese di personale	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: Spese di infrastruttura e funzionamento	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Spese operative	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Totale (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Spese di personale	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Spese di infrastruttura e funzionamento	0	0	0	0	0	0	0	0	0	0
T3: Spese operative	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Totale (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18.02.05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Spese di personale	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Spese di infrastruttura e funzionamento	0	0	0	0	0	0	0	0	0	0
T3: Spese operative	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Totale (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex - EBCG										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total(formula)**
T1: Spese di personale	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: Spese di infrastruttura e funzionamento	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: Spese operative	0	0	0	0,183	2,200	0	0	0	0	2,383
Totale (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
TOTALE (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. DG HOME Rubrica 5 "spese amministrative"										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Totale (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTALE (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale.

3.2.6. Partecipazione di terzi al finanziamento

– La proposta/iniziativa non prevede cofinanziamenti da terzi.

3.3. Incidenza prevista sulle entrate

– ☐ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☒ La proposta/iniziativa ha la seguente incidenza finanziaria:

– – ☐ sulle risorse proprie

– – ☒ sulle entrate varie

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[100]								
		Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**	Anno **2023**	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**
Articolo 6313 - Contributo degli Stati associali Schengen (CH, NO, LI, IS)……		pm	pm	pm	pm	pm	pm	pm	pm	pm

Per quanto riguarda le entrate varie con destinazione specifica, precisare la o le linee di spesa interessate.

18.0207

Precisare il metodo di calcolo dell'incidenza sulle entrate.

Il bilancio comprenderà un contributo da parte dei paesi associati all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen e alle misure relative a Eurodac, conformemente ai rispettivi accordi.

[100] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 25% per spese di riscossione.