



Consiglio
dell'Unione europea

Bruxelles, 9 dicembre 2021
(OR. en)

14204/21

**Fascicolo interistituzionale:
2021/0410(COD)**

**IXIM 259
ENFOPOL 459
JAI 1278
CODEC 1518
IA 201**

PROPOSTA

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	9 dicembre 2021
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2021) 784 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II"), che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio

Si trasmette in allegato, per le delegazioni, il documento COM(2021) 784 final.

All: COM(2021) 784 final



COMMISSIONE
EUROPEA

Bruxelles, 8.12.2021
COM(2021) 784 final

2021/0410 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II"), che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio

{SEC(2021) 421 final} - {SWD(2021) 378 final} - {SWD(2021) 379 final}

RELAZIONE

CONTESTO DELLA PROPOSTA

- **Motivi della proposta**

In tutta Europa la criminalità mina la sicurezza e il benessere dei cittadini dell'UE. Le autorità di contrasto necessitano di strumenti solidi e performanti per contrastarla in maniera efficace. La cooperazione e lo scambio di informazioni sono gli strumenti più efficaci per combattere la criminalità e far applicare la legge¹. Nel 2021 è stato riscontrato che oltre il 70 % dei gruppi della criminalità organizzata è presente in più di tre Stati membri². Anche la criminalità avente apparentemente natura più locale può avere legami con altri luoghi in Europa nei quali il medesimo autore del reato ha compiuto atti criminali. Analogamente i legami della presunta criminalità locale con strutture e operazioni della criminalità organizzata spesso non sono evidenti. Di conseguenza, per poter contrastare efficacemente la criminalità le autorità di contrasto devono potersi scambiare tra loro dati in maniera tempestiva. L'UE ha già fornito alle forze di contrasto una serie di strumenti destinati a facilitare lo scambio di informazioni, che si sono dimostrati fondamentali per scoprire attività e reti criminali³, ma rimangono da colmare alcune carenze di informazioni. In considerazione del fatto che i dati vengono archiviati separatamente in vari sistemi informatici nazionali e sistemi informatici su larga scala a livello dell'UE, occorre assicurare che i sistemi siano in grado di comunicare tra loro.

In uno spazio senza controlli alle frontiere interne (lo "spazio Schengen"), persistono comunque confini e ostacoli per quanto riguarda lo scambio di dati tra autorità di contrasto⁴, e pertanto rimangono zone d'ombra e lacune di cui approfittano numerosi criminali e terroristi che agiscono in più Stati membri. La presente iniziativa, unitamente alla proposta, adottata in parallelo, relativa a una direttiva sullo scambio di informazioni tra le autorità di contrasto degli Stati membri⁵, mira a rafforzare lo scambio di informazioni tra gli Stati membri e quindi fornire alle autorità di contrasto dell'UE strumenti potenziati per combattere la criminalità e il terrorismo⁶.

Da più di dieci anni il quadro Prüm consente alle autorità di contrasto in tutta l'UE di scambiarsi informazioni. Le decisioni Prüm⁷, adottate nel 2008 con l'obiettivo di sostenere la cooperazione giudiziaria e di polizia a livello transfrontaliero in relazione a questioni penali, prevedono lo scambio automatizzato di dati specifici (dati relativi a profili DNA, impronte digitali e immatricolazione di veicoli) tra le autorità competenti per la prevenzione, l'indagine e l'accertamento di reati. Il quadro Prüm sta contribuendo con successo alla lotta alla criminalità e al terrorismo nell'UE, ma restano comunque lacune nel settore dello scambio di informazioni e pertanto vi è margine per ulteriori miglioramenti.

¹ Cfr. "Strategia dell'UE per l'Unione della sicurezza", COM(2020) 605 final del 24.7.2020.

² *Valutazione dell'UE della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità 2021*.

³ Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025, COM(2021) 170 final del 14.4.2021.

⁴ Ad esempio le modalità di scambio di talune categorie di dati, il canale utilizzato per tali scambi, i termini applicabili, ecc.

⁵ [Riferimento].

⁶ Comunicazione della Commissione, Strategia per uno spazio Schengen senza controlli alle frontiere interne pienamente funzionante e resiliente, COM(2021) 277 final del 2.6.2021.

⁷ La decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, e la decisione 2008/616/GAI del Consiglio, del 23 giugno 2008, relativa all'attuazione della decisione 2008/615/GAI. Le decisioni del Consiglio si basano sulla convenzione di Prüm del 2005.

Le conclusioni del Consiglio sull'attuazione delle decisioni Prüm a dieci anni dall'adozione hanno sottolineato l'importanza della consultazione e del confronto automatizzati di profili DNA, dati dattiloscopici e dati di immatricolazione dei veicoli, per far fronte al terrorismo e alla criminalità transfrontaliera. Il Consiglio ha altresì invitato la Commissione a considerare l'eventualità di una revisione delle decisioni Prüm allo scopo di estenderne l'ambito di applicazione e di aggiornare i requisiti tecnici e giuridici necessari⁸.

Il quadro Prüm II si basa sull'attuale quadro Prüm, rafforzando e modernizzando tale quadro e consentendo l'interoperabilità con altri sistemi di informazione dell'UE. Garantirà che tutti i dati pertinenti disponibili per le autorità di contrasto in uno Stato membro possano essere utilizzati dalle autorità di contrasto in altri Stati membri. Garantirà altresì che l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) possa fornire sostegno agli Stati membri nel contesto del quadro Prüm. La presente iniziativa prevede la creazione di una nuova architettura che consenta uno scambio più facile e più rapido di dati tra Stati membri e che garantisca un livello elevato di protezione dei diritti fondamentali.

- **Obiettivi della proposta**

L'obiettivo generale della presente iniziativa deriva dall'obiettivo del trattato di contribuire alla sicurezza interna dell'Unione europea. Tra le misure per procedere in tal senso figurano la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni⁹. L'obiettivo generale di questo strumento consiste quindi nel migliorare, semplificare e facilitare lo scambio di informazioni a fini di prevenzione, indagine e accertamento di reati, anche di terrorismo, tra le autorità di contrasto degli Stati membri, ma anche con Europol, in veste di polo centrale dell'UE per le informazioni sulla criminalità.

Gli obiettivi strategici specifici della presente proposta sono:

- (a) fornire una soluzione tecnica per uno scambio automatizzato di dati efficiente tra le autorità di contrasto affinché vengano a conoscenza dei dati pertinenti disponibili nella banca dati nazionale di un altro Stato membro;
- (b) garantire che i dati più pertinenti (in termini di categorie di dati) delle banche dati nazionali di altri Stati membri siano messi a disposizione di tutte le autorità di contrasto competenti;
- (c) garantire che i dati pertinenti (in termini di fonti di dati) delle banche dati di Europol siano messi a disposizione delle autorità di contrasto;
- (d) fornire alle autorità di contrasto un accesso efficiente ai dati effettivi corrispondenti a un "hit" (riscontro positivo) disponibile nella banca dati nazionale di un altro Stato membro.

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

La recente strategia Schengen¹⁰ ha annunciato diverse misure destinate a intensificare la cooperazione di polizia e lo scambio di informazioni tra le autorità di contrasto al fine di rafforzare la sicurezza in uno spazio intrinsecamente interdipendente senza frontiere interne. Unitamente alla proposta di direttiva sullo scambio di informazioni tra le autorità di contrasto degli Stati membri, la presente

⁸ Conclusioni del Consiglio sull'attuazione delle "DECISIONI PRÜM" a dieci anni dall'adozione (documento 11227/18), <https://data.consilium.europa.eu/doc/document/ST-11227-2018-INIT/it/pdf>.

⁹ Articolo 87, paragrafo 2, lettera a), TFUE.

¹⁰ Comunicazione della Commissione al Parlamento europeo e al Consiglio, "Strategia per uno spazio Schengen senza controlli alle frontiere interne pienamente funzionante e resiliente", COM(2021) 277 final del 2.6.2021.

proposta contribuisce agli obiettivi di tale strategia garantendo che le autorità di contrasto di uno Stato membro abbiano accesso alle stesse informazioni a disposizione dei loro colleghi in un altro Stato membro.

La proposta si inserisce nel contesto di più ampia portata dei sistemi di informazione su larga scala dell'UE che si è sviluppato in modo sostanziale dopo l'adozione del quadro Prüm. In tale contesto figurano i tre sistemi centrali di informazione dell'UE attualmente in funzione: il sistema d'informazione Schengen (SIS), il sistema d'informazione visti (VIS) e il sistema Eurodac¹¹. Sono inoltre attualmente in fase di sviluppo tre sistemi nuovi, ossia: il sistema di ingressi/uscite (EES), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e il sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN)¹². Tutti questi sistemi attuali e futuri sono collegati attraverso il quadro per l'interoperabilità tra i sistemi di informazione dell'UE¹³ per la sicurezza, le frontiere e la gestione della migrazione, adottato nel 2019 e attualmente in fase di attuazione. Le revisioni incluse nella presente proposta mirano ad allineare il quadro Prüm al quadro per l'interoperabilità, in particolare per quanto concerne lo scambio di dati e l'architettura complessiva offerta dall'interoperabilità dei sistemi di informazione dell'UE. Risulterebbe così possibile un accesso rapido e controllato alle informazioni di cui gli operatori delle autorità di contrasto necessitano per svolgere i propri compiti e per le quali dispongono di diritti di accesso.

Il SIS contiene già segnalazioni di persone scomparse e consente ricerche basate sulle impronte digitali. Il SIS è un sistema di informazione centralizzato che consente di intraprendere azioni sulla base di un meccanismo di tipo "hit/no hit" (riscontro positivo/riscontro negativo), direttamente accessibile a un gran numero di utenti finali operanti in prima linea, che contiene segnalazioni e fornisce una risposta immediata in loco, offrendo la possibilità di intraprendere azioni in relazione all'oggetto della segnalazione. Il SIS è utilizzato principalmente in occasione di controlli di polizia, di frontiera e doganali, nonché dalle autorità competenti per i visti e per l'immigrazione nelle loro procedure e verifiche abituali.

Al contrario il quadro Prüm non dispone di alcuna componente/banca dati a livello dell'UE ed è utilizzato soltanto nelle indagini penali. Consente ad altri Stati membri di accedere ai sottoinsiemi anonimizzati delle banche dati nazionali sui profili DNA e sulle impronte digitali di autori di reati di tutti gli Stati membri collegati. Tale accesso è consentito soltanto ai punti di contatto nazionali. Sebbene la risposta "hit/no hit" venga fornita in pochi secondi o minuti, potrebbero essere necessarie settimane o addirittura mesi per ricevere i dati personali corrispondenti relativi a un riscontro positivo.

¹¹ Il SIS fornisce assistenza alle autorità competenti dell'UE nel preservare la sicurezza interna in assenza di controlli alle frontiere interne, mentre il VIS consente agli Stati Schengen di scambiarsi dati sui visti. Il sistema Eurodac istituisce una banca dati dell'UE per le impronte digitali dei richiedenti asilo che consente agli Stati membri di confrontare le impronte digitali dei richiedenti asilo per verificare se abbiano precedentemente chiesto asilo o siano entrati nell'UE in modo irregolare attraverso un altro Stato membro.

¹² L'EES e l'ETIAS rafforzeranno i controlli di sicurezza sui viaggiatori esentati dall'obbligo del visto consentendo verifiche preventive in materia di migrazione irregolare e sicurezza. Il sistema ECRIS-TCN affronterà la lacuna individuata nello scambio di informazioni tra Stati membri in merito a cittadini di paesi terzi condannati.

¹³Regolamenti del Parlamento europeo e del Consiglio (UE) 2019/817 e (UE) 2019/818.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

• Base giuridica

La base giuridica della presente proposta di regolamento è costituita dalle disposizioni seguenti del trattato sul funzionamento dell'Unione europea (TFUE): articolo 16, paragrafo 2, articolo 87, paragrafo 2, lettera a), e articolo 88, paragrafo 2.

A norma dell'articolo 16, paragrafo 2, l'Unione è competente a stabilire le norme 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. A norma dell'articolo 87, paragrafo 2, lettera a), l'Unione ha il potere di stabilire misure riguardanti la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni al fine di garantire la cooperazione di polizia tra le autorità competenti degli Stati membri, compresi i servizi di polizia, delle dogane e altri servizi incaricati dell'applicazione della legge specializzati nel settore della prevenzione o dell'individuazione dei reati e delle relative indagini. A norma dell'articolo 88, paragrafo 2, il Parlamento europeo e il Consiglio possono determinare la struttura, il funzionamento, la sfera d'azione e i compiti di Europol.

• Sussidiarietà

Il miglioramento dello scambio di informazioni tra la polizia e le autorità di contrasto all'interno dell'UE non può essere realizzato in misura sufficiente dagli Stati membri in maniera isolata, in ragione della natura transfrontaliera della lotta alla criminalità e delle questioni di sicurezza. In tali settori gli Stati membri devono fare affidamento gli uni sugli altri.

Attraverso diversi progetti di attuazione a livello UE¹⁴, gli Stati membri hanno cercato di intervenire per affrontare le carenze dell'attuale quadro Prüm¹⁵. Nonostante tutte queste azioni, molte carenze sono rimaste le medesime descritte nella relazione del 2012 sull'attuazione della decisione Prüm¹⁶. Ciò dimostra la necessità di un'azione a livello di UE, in quanto le misure attuate dai soli Stati membri non si sono dimostrate sufficienti per affrontare i limiti del quadro Prüm attuale.

Regole, norme e requisiti comuni a livello di UE facilitano inoltre gli scambi di informazioni garantendo al tempo stesso la compatibilità tra i diversi sistemi nazionali. Ciò a sua volta consente un certo livello di automazione nei flussi di lavoro dello scambio di informazioni, che libera gli operatori delle autorità di contrasto da attività manuali ad elevata intensità di lavoro.

¹⁴ Ad esempio, il progetto *Mobile Competence Team* (MCT) (2011–2014) è stato avviato dalla Germania e finanziato dal programma "Prevenzione e lotta contro la criminalità" (ISEC) della Commissione. L'MCT mirava a fornire conoscenze specialistiche e sostegno agli Stati membri dell'UE che non erano ancora operativi in materia di scambio di dati in merito a DNA e impronte digitali.

¹⁵ Attraverso un progetto guidato dalla Finlandia, gli Stati membri hanno analizzato le procedure nazionali applicate a seguito di un riscontro positivo. In base all'esito di tale progetto è stata raccomandata una serie di buone pratiche non obbligatorie destinate a semplificare lo scambio di informazioni in seguito a un riscontro positivo in tutta l'UE (cfr. documento 14310/2/16 REV2, non pubblico).

Nel 2012-2013, Europol ha sostenuto lo sviluppo di moduli standardizzati da utilizzare per lo scambio di informazioni di follow-up, indipendentemente dal canale di comunicazione utilizzato (cfr. documento 9383/13 per ulteriori informazioni). Tuttavia non è noto in quale misura i punti di contatto nazionali utilizzino tali moduli.

¹⁶COM(2012) 732 final.

- **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 in quanto non vanno al di là di quanto necessario per il conseguimento degli obiettivi individuati.

La proposta prevede la creazione di **router centrali** (il router Prüm II ed EPRIS) che fungerebbero ciascuno da punto di connessione tra gli Stati membri. Si tratta di un approccio ibrido tra una soluzione decentrata e una centralizzata, senza alcuna archiviazione di dati a livello centrale. Ciò implica che le banche dati nazionali in ciascuno Stato membro si collegheranno tutte al router centrale anziché connettersi tra di loro. Tali router fungerebbero da intermediari di messaggi che inoltrano le operazioni di consultazione e le risposte ai sistemi nazionali, senza creare nuove elaborazioni di dati, ampliare i diritti di accesso né sostituire le banche dati nazionali. L'approccio garantirebbe alle autorità di contrasto un accesso rapido e controllato alle informazioni di cui necessitano per svolgere i loro compiti, in linea con i diritti di accesso di cui godono. Il router faciliterebbe l'attuazione da parte degli Stati membri degli scambi di dati esistenti e futuri nel contesto del quadro Prüm.

Lo **scambio automatizzato di categorie di dati complementari**, quali immagini del volto e estratti del casellario giudiziale, è fondamentale per l'efficacia delle indagini penali e per identificare i criminali. L'introduzione di tali categorie di dati complementari non richiederebbe la conservazione di nuove categorie di dati, dato che gli Stati membri già li raccolgono ai sensi del diritto nazionale e li conservano nelle banche dati nazionali. Lo scambio di tali nuove categorie di dati costituirebbe un nuovo trattamento dei dati. Tuttavia sarebbe limitato alla misura necessaria per il conseguimento della sua finalità e consentirebbe il confronto dei dati soltanto caso per caso. La proposta prevede altresì una serie di diverse garanzie (ad esempio la condivisione di tutti i dati soltanto in presenza di un riscontro positivo a seguito di un'interrogazione).

Tramite la presente proposta **Europol** formerà parte integrante del quadro Prüm, innanzitutto perché consentirà agli Stati membri di controllare automaticamente i dati biometrici provenienti da paesi terzi conservati presso Europol, in secondo luogo perché potrebbe confrontare i dati provenienti da paesi terzi con le banche dati nazionali degli Stati membri. Questi due aspetti della partecipazione di Europol al nuovo quadro Prüm, in conformità con i compiti attribuiti a Europol dal regolamento (UE) 2016/794, permetterebbero di evitare lacune in relazione ai dati concernenti reati gravi e reati di terrorismo ricevuti da paesi terzi. In una società aperta, in un mondo globalizzato, i dati forniti da paesi terzi su criminali e terroristi sono fondamentali. Ciò consentirebbe la potenziale identificazione di criminali noti a paesi al di fuori dell'UE, mantenendo al tempo stesso le solide garanzie in materia di protezione della vita privata e dei diritti e delle libertà fondamentali delle persone fisiche previste dagli accordi di cooperazione di Europol con paesi terzi.

Il **processo** riveduto **di scambio di follow-up sui riscontri positivi** contribuirebbe alla sicurezza interna dell'Unione europea semplificando e ottimizzando lo scambio di informazioni in materia di contrasto. Rispetto alla situazione attuale, nella quale lo scambio di informazioni a seguito di un riscontro positivo è disciplinato dal diritto nazionale ed è quindi soggetto a norme e procedure diverse, l'introduzione di norme comuni che armonizzino questa seconda fase del processo Prüm offrirebbe prevedibilità a tutti gli utenti, dato che tutti saprebbero quali dati otterrebbero in tale fase. Lo scambio di dati sarebbe facilitato da un'automazione parziale, il che significa che sarebbe comunque necessario l'intervento umano prima che possa aver luogo uno scambio completo di dati supplementari. Gli Stati membri manterrebbero la proprietà/il controllo dei propri dati.

- **Scelta dell'atto giuridico**

L'atto giuridico proposto è un regolamento del Parlamento europeo e del Consiglio. La normativa proposta si fonda su un quadro esistente di decisioni del Consiglio che contribuiscono alla cooperazione transfrontaliera tra gli Stati membri dell'UE nei settori della giustizia e degli affari interni¹⁷.

In considerazione della necessità che le misure proposte siano direttamente applicabili e applicate uniformemente in tutti gli Stati membri, nonché di rafforzare lo scambio di informazioni, un regolamento costituisce quindi la scelta adeguata in termini di strumento giuridico.

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

- **Valutazioni ex post della legislazione vigente**

Nel complesso dalla valutazione del quadro Prüm¹⁸ è emerso che la consultazione e il raffronto di dati relativi a DNA, impronte digitali e immatricolazione di veicoli nelle banche dati di altri Stati membri ai fini della prevenzione dei reati e delle indagini penali sono di fondamentale importanza per proteggere la sicurezza interna dell'UE e la sicurezza dei suoi cittadini. Tale valutazione ha altresì dimostrato che le decisioni Prüm hanno contribuito a stabilire regole, norme e requisiti comuni a livello UE, al fine di facilitare lo scambio di informazioni e garantire la compatibilità tra i diversi sistemi nazionali.

Tuttavia, dopo la scadenza del termine per l'attuazione del quadro Prüm dieci anni fa, l'UE ha adottato diverse altre misure sull'agevolazione dello scambio di informazioni tra le autorità di contrasto¹⁹, compreso il quadro per l'interoperabilità²⁰. Inoltre le disposizioni sulle specifiche tecniche di interrogazioni, misure di sicurezza e comunicazione non sono state aggiornate sin dall'adozione delle decisioni Prüm nel 2008²¹. Talune di tali norme sono obsolete dato che la scienza forense e le tecnologie si sono sviluppate in modo significativo nell'ultimo decennio.

Dalla valutazione è emerso altresì che l'attuazione delle decisioni Prüm negli ultimi dieci anni è stata lenta e che non tutti gli Stati membri hanno adottato le misure necessarie per attuare le decisioni²². Di conseguenza numerose connessioni bilaterali non sono state stabilite e non è possibile avviare interrogazioni per le banche dati di taluni Stati membri. Dalle conclusioni della valutazione è emerso

¹⁷ La decisione 2008/615/GAI del Consiglio sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, e la decisione 2008/616/GAI del Consiglio, relativa all'attuazione della decisione 2008/615/GAI.

¹⁸ Allegato 4 del documento di lavoro dei servizi della Commissione che accompagna la proposta [riferimento alla valutazione d'impatto Prüm].

¹⁹ Come il sistema di informazione Europol (EIS), i sistemi di informazione Interpol e il sistema d'informazione Schengen (SIS).

²⁰ Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio;

regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816.

²¹ Di cui alla decisione 2008/616/GAI del Consiglio.

²² Nel 2016 la Commissione ha avviato procedure di infrazione contro cinque Stati membri. Ad ottobre 2021 due di tali casi di infrazione sono ancora aperti.

altresi che il seguito dato a un riscontro positivo si svolge sulla base del diritto nazionale e, pertanto, esula dall'ambito di applicazione delle decisioni Prüm. A causa delle differenze tra le norme e le procedure nazionali, in diversi casi le autorità competenti possono ricevere con notevole ritardo le informazioni a seguito di un riscontro positivo. Tale situazione attuale incide sul funzionamento del sistema Prüm e sullo scambio efficace di informazioni tra gli Stati membri, diminuendo la possibilità di identificare i criminali e di individuare i collegamenti transfrontalieri tra reati.

I risultati della valutazione hanno sostenuto la preparazione della valutazione d'impatto e della presente proposta.

- **Consultazioni dei portatori di interessi**

La preparazione della presente proposta ha comportato consultazioni mirate dei portatori di interessi, fra cui gli utenti finali del sistema, in particolare le autorità degli Stati membri che utilizzano lo scambio automatizzato di dati del quadro Prüm, le quali spaziano dalle autorità di contrasto e giudiziarie alle autorità nazionali competenti per l'immatricolazione dei veicoli, fino ai custodi di banche dati nazionali e ai laboratori forensi. Sono state consultate altresì Europol e l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) in considerazione delle rispettive competenze e del loro ruolo potenziale nel nuovo quadro Prüm.

In ragione delle loro competenze, contributi sono stati forniti anche dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA), così come da organizzazioni non governative quali EDRi (European Digital Rights) e da organizzazioni intergovernative (Eucaris, il sistema europeo d'informazione sui veicoli e le patenti di guida).

Le attività di consultazione nel contesto della preparazione della valutazione d'impatto alla base della presente proposta hanno raccolto riscontri dai portatori di interessi in vari consessi. Tali attività hanno compreso in particolare una valutazione d'impatto iniziale, una consultazione pubblica e una serie di seminari tecnici. È stato condotto uno studio di fattibilità basato su ricerche documentali, colloqui con esperti in materia, questionari e tre seminari di esperti, che ha esaminato la fattibilità del miglioramento dello scambio di informazioni ai sensi delle decisioni Prüm.

Discussioni regolari sullo scambio di informazioni in materia di contrasto e in particolare sulle decisioni Prüm in seno al gruppo di lavoro del Consiglio DAPIX/IXIM²³ hanno contribuito anch'esse alla preparazione della presente proposta.

Al fine di raccogliere riscontri, da agosto a ottobre del 2020 è stata pubblicata una **valutazione d'impatto iniziale**, in relazione alla quale sono pervenuti complessivamente sei contributi²⁴.

Una **consultazione pubblica** pubblicizzata sul sito web della Commissione europea è stata rivolta al pubblico in generale. Le risposte hanno confermato che il quadro Prüm attualmente in vigore è pertinente per la prevenzione dei reati e le indagini penali e ha migliorato lo scambio di dati tra le autorità di contrasto degli Stati membri. Evitando la necessità di interrogare ciascuno Stato membro a livello bilaterale, lo scambio automatizzato di dati nel quadro Prüm ha consentito altresì di migliorare l'efficienza. Le risposte hanno confermato ulteriormente che il quadro Prüm è coerente con le azioni

²³ Gruppo di lavoro del Consiglio "Scambio di informazioni e protezione dei dati" (DAPIX) e, dal 1° gennaio 2020, gruppo di lavoro "Scambio di informazioni nel settore della giustizia e degli affari interni" (IXIM).

²⁴La valutazione d'impatto iniziale e i contributi sono disponibili a [questo indirizzo](#).

dell'UE e internazionali in questo settore e che presenta un valore aggiunto rispetto a quanto gli Stati membri potrebbero conseguire nel settore dello scambio di informazioni in materia di contrasto in mancanza di tale quadro. In termini di rafforzamento del quadro attualmente in vigore, la maggior parte dei partecipanti ha convenuto che il fatto che alcune categorie di dati non siano oggetto del quadro e siano quindi scambiate mediante l'invio di interrogazioni manuali costituisce una lacuna.

I servizi della Commissione hanno organizzato altresì una serie di **seminari tecnici** informali mirati con esperti degli Stati membri e dei paesi associati Schengen. Tali seminari miravano a riunire gli utenti finali per uno scambio di opinioni, da un punto di vista tecnico, sulle opzioni che erano state previste e valutate per rafforzare il quadro Prüm.

La valutazione d'impatto che accompagna la presente proposta riporta una descrizione più dettagliata della consultazione dei portatori di interesse (allegato 2).

- **Valutazione d'impatto**

La presente proposta è corredata di una valutazione d'impatto, presentata nel documento di lavoro dei servizi della Commissione [riferimento alla valutazione d'impatto Prüm] che la accompagna. Il comitato per il controllo normativo ha riesaminato il progetto di valutazione d'impatto nella riunione del 14 luglio 2021 e ha espresso un parere positivo il 16 luglio 2021.

La valutazione ha concluso che:

- (1) al fine di conseguire l'obiettivo di fornire una soluzione tecnica per uno scambio automatizzato di dati efficiente, dovrebbe essere applicata una soluzione ibrida tra un approccio decentrato e un approccio centralizzato senza conservazione di dati a livello centrale;
- (2) al fine di conseguire l'obiettivo di garantire che i dati più pertinenti (in termini di categorie di dati) siano disponibili per le autorità di contrasto, dovrebbe essere introdotto lo scambio di immagini del volto e di estratti del casellario giudiziale;
- (3) al fine di conseguire l'obiettivo di garantire che i dati pertinenti delle banche dati di Europol siano a disposizione delle autorità di contrasto, gli Stati membri dovrebbero essere in grado di controllare automaticamente i dati biometrici provenienti da paesi terzi presso Europol nel contesto del quadro Prüm. Europol dovrebbe altresì essere in grado di confrontare i dati provenienti da paesi terzi con le banche dati nazionali degli Stati membri;
- (4) al fine di conseguire l'obiettivo di fornire un accesso efficiente ai dati effettivi corrispondenti a un "hit" (riscontro positivo) disponibili nella banca dati nazionale di un altro Stato membro o presso Europol, il processo di follow-up dovrebbe essere disciplinato a livello dell'UE con uno scambio semiautomatico dei dati effettivi corrispondenti a un "hit".

L'impatto positivo principale della presente proposta sarà quello di rispondere efficacemente ai problemi individuati e rafforzare l'attuale quadro Prüm con forti capacità aggiuntive destinate a fornire maggiore sostegno agli Stati membri nell'intensificare lo scambio di informazioni, con l'obiettivo finale di prevenire e indagare reati, anche di terrorismo, nel pieno rispetto dei diritti fondamentali.

I beneficiari finali di tutte le opzioni prescelte sono i cittadini, che beneficeranno direttamente e indirettamente di un migliore contrasto della criminalità e di una diminuzione dei tassi di criminalità. In termini di efficienza, i beneficiari principali sono le autorità di contrasto nazionali.

Gli effetti finanziari ed economici immediati della proposta richiederanno investimenti a livello tanto di UE quanto di Stati membri. I costi degli investimenti previsti dovrebbero essere controbilanciati dai benefici e dai risparmi, in particolare a livello di Stati membri. Nonostante gli investimenti iniziali, la creazione del router centrale Prüm consentirà risparmi sui costi sostenuti dagli Stati membri, dato che non sarebbe richiesto a ciascuno Stato membro di creare (e gestire) tante connessioni quanti sono gli Stati membri e le categorie di dati.

- **Diritti fondamentali**

Conformemente alla Carta dei diritti fondamentali dell'Unione europea, che vincola tanto le istituzioni dell'UE quanto gli Stati membri nell'attuazione del diritto dell'Unione (articolo 51, paragrafo 1, della Carta), e al principio di non discriminazione, le opportunità offerte dalle opzioni presentate devono conciliarsi con l'obbligo di garantire che le ingerenze nei diritti fondamentali eventualmente generate da tali opportunità 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 proposte offrono la possibilità di adottare misure preventive mirate, allo scopo di aumentare la sicurezza. Di conseguenza possono contribuire a perseguire l'obiettivo legittimo di agevolare la lotta alla criminalità, che implica altresì un obbligo positivo per le autorità di adottare misure operative preventive per proteggere una persona la cui vita sia a rischio, qualora siano a conoscenza o avrebbero dovuto essere a conoscenza dell'esistenza di un rischio immediato²⁵.

- **Protezione dei dati personali**

Lo scambio di informazioni incide sul diritto alla protezione dei dati personali. 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 europea²⁶, il diritto alla protezione dei dati personali non appare come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale. La protezione dei dati è strettamente legata al rispetto della vita privata e familiare tutelato dall'articolo 7 della Carta.

Per quanto concerne il quadro Prüm, la normativa in materia di protezione dei dati applicabile è la direttiva (UE) 2016/680. Il quadro Prüm prevede infatti il trattamento di dati personali effettuato nel contesto dello scambio di informazioni tra le autorità di contrasto competenti per la prevenzione dei reati e le indagini penali.

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:

- (1) devono essere previste dalla legge;
- (2) devono rispettare il contenuto essenziale dei diritti;

²⁵ Corte europea dei diritti dell'uomo, *Salih Osman contro Regno Unito*, sentenza n. 87/1997/871/1083, del 28 ottobre 1998, punto 116.

²⁶ Sentenza della Corte di giustizia dell'Unione europea del 9.11.2010, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*, cause riunite C-92/09 e C-93/09, Racc. 2010, pag. I-0000.

- (3) devono rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui;
- (4) devono essere necessarie; e
- (5) 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". 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 del quadro Prüm riveduto ed è limitato alla misura in cui tali dati sono necessari per eseguire i compiti connessi al conseguimento degli scopi predetti.

Al momento in cui sarà pubblicata la relazione che valuta l'attuazione della [raccomandazione del Consiglio sulla cooperazione operativa di polizia] da parte degli Stati membri di cui al punto 9, lettera d), di tale raccomandazione, la Commissione deciderà se sia necessario un atto normativo dell'UE sulla cooperazione operativa transfrontaliera tra le forze di polizia. Se fosse necessario, la Commissione presenterà una proposta legislativa sulla cooperazione operativa transfrontaliera di polizia, che garantirà anche l'allineamento delle disposizioni della decisione 2008/615/GAI e della decisione 2008/616/GAI non contemplate dalla presente proposta con la direttiva (UE) 2016/680, in funzione dei risultati della valutazione di cui all'articolo 62, paragrafo 6, della direttiva (UE) 2016/680. Se invece non fosse necessaria una normativa UE sulla cooperazione operativa transfrontaliera di polizia, la Commissione presenterà una proposta legislativa per garantire lo stesso allineamento, in funzione dei risultati della valutazione di cui all'articolo 62, paragrafo 6, della direttiva (UE) 2016/680.

4. INCIDENZA SUL BILANCIO

La presente iniziativa legislativa inciderebbe sul bilancio e sul fabbisogno di personale di eu-LISA ed Europol.

Per eu-LISA, si stima che sarebbe necessario un bilancio aggiuntivo di circa 16 milioni di EUR e circa 10 posti aggiuntivi per il periodo complessivo del quadro finanziario pluriennale (QFP) affinché eu-LISA disponga delle risorse necessarie per far rispettare i compiti attribuiti all'agenzia nel contesto della presente proposta di regolamento. Il bilancio assegnato a eu-LISA sarà compensato dallo Strumento di sostegno finanziario per la gestione delle frontiere e la politica dei visti.

Per Europol, si stima che sarebbe necessario un bilancio aggiuntivo di circa 7 milioni di EUR e circa 5 posti aggiuntivi per il periodo complessivo del QFP affinché Europol disponga delle risorse necessarie per far rispettare i compiti attribuiti all'agenzia nel contesto della presente proposta di regolamento. Il bilancio assegnato a eu-LISA sarà compensato dal Fondo sicurezza interna.

5. ALTRI ELEMENTI

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

La Commissione assicurerà che siano in atto le disposizioni necessarie per monitorare il funzionamento delle misure proposte e valutarle rispetto ai principali obiettivi strategici. Due anni dopo la messa in atto e in servizio delle nuove funzionalità e, in seguito, ogni due anni, le Agenzie dell'Unione

dovrebbero presentare al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico delle nuove misure proposte. Inoltre, tre anni dopo l'introduzione e l'avvio operativo delle nuove funzionalità e, in seguito, ogni quattro anni, la Commissione dovrebbe predisporre una valutazione generale delle misure, anche in merito alla loro eventuale incidenza diretta o indiretta sui diritti fondamentali. Essa dovrebbe esaminare i risultati conseguiti rispetto agli obiettivi, valutando nel contempo se i principi di base siano 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 1 stabilisce le disposizioni generali del presente regolamento indicandone l'oggetto, la finalità e l'ambito di applicazione. Fornisce un elenco di definizioni e ricorda che il trattamento dei dati personali ai fini del presente regolamento deve rispettare il principio di non discriminazione e altri diritti fondamentali.

Il capo 2 stabilisce le disposizioni applicabili allo scambio delle categorie di dati previste dal presente regolamento, ossia profili DNA, dati dattiloscopici, dati di immatricolazione dei veicoli, immagini del volto ed estratti del casellario giudiziale. I principi su cui devono basarsi lo scambio e la consultazione automatizzata dei dati, le regole per le domande e le risposte sono illustrati rispettivamente in una sezione distinta per ciascuna categoria di dati. Il capo 2 contiene altresì disposizioni comuni per lo scambio di dati, l'istituzione di punti di contatto nazionali e misure di attuazione.

Il capo 3 definisce i dettagli della nuova architettura (tecnica) per lo scambio di dati. La prima sezione di tale capo comprende disposizioni che descrivono il router centrale, il suo uso e l'avvio di interrogazioni. Saranno necessari atti di esecuzione per specificare le procedure tecniche relative a tali interrogazioni. Questa sezione comprende altresì disposizioni sull'interoperabilità tra il router e l'archivio comune di dati di identità ai fini dell'accesso da parte delle autorità di contrasto, la registrazione di tutti i trattamenti di dati nel router, il controllo di qualità nonché le procedure di notifica in caso di impossibilità tecnica di utilizzare il router. Una seconda sezione fornisce dettagli sull'utilizzo dell'indice europeo dei casellari giudiziali (EPRIS) per lo scambio dei relativi estratti. Questa sezione include altresì disposizioni sulla registrazione di tutte le operazioni di trattamento di dati in EPRIS nonché sulle procedure di notifica in caso di impossibilità tecnica di utilizzare EPRIS.

Il capo 4 definisce i processi per lo scambio di dati a seguito di una corrispondenza riscontrata. Comprende una disposizione sullo scambio automatizzato di dati di base, secondo cui i dati devono essere limitati a quanto necessario per consentire l'identificazione della persona interessata, e una disposizione sullo scambio di dati effettuato in qualsiasi fase del processo in conformità del regolamento che non sia esplicitamente descritto nel regolamento stesso.

Il capo 5 contiene disposizioni sull'accesso da parte degli Stati membri ai dati biometrici provenienti da paesi terzi conservati da Europol e sull'accesso da parte di Europol ai dati conservati nelle banche dati degli Stati membri.

Il capo 6, sulla protezione dei dati, contiene disposizioni destinate ad assicurare che i dati trattati in conformità del presente regolamento siano trattati in modo lecito e adeguato, in linea con le disposizioni della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro

2008/977/GAI del Consiglio²⁷. Spiega chi sarà il responsabile del trattamento dei dati in conformità del presente regolamento. Stabilisce le misure richieste da eu-LISA e dalle autorità degli Stati membri per garantire la sicurezza del trattamento dei dati, la gestione adeguata degli incidenti di sicurezza e il monitoraggio del rispetto delle misure del presente regolamento. Questo capo contiene infine disposizioni riguardanti la vigilanza e l'audit in relazione alla protezione dei dati. Sottolinea il principio secondo cui i dati trattati ai sensi del presente regolamento non devono essere trasferiti o messi a disposizione di alcun paese terzo od organizzazione internazionale in maniera automatizzata.

Il capo 7 illustra in dettaglio le rispettive competenze degli Stati membri, di Europol e di eu-LISA nell'attuazione delle misure previste dal regolamento.

Il capo 8 riguarda le modifiche di altri strumenti esistenti, ossia le decisioni 2008/615/GAI e 2008/616/GAI e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818.

Il capitolo 9 sulle disposizioni finali definisce i dettagli relativi a relazioni e statistiche, costi, notifiche, disposizioni transitorie e deroghe. Fissa altresì le prescrizioni per l'entrata in funzione delle misure proposte nel contesto del presente regolamento. Questo capo prevede inoltre l'istituzione di un comitato e l'adozione di un manuale pratico a supporto dell'attuazione e della gestione del presente regolamento. Comprende inoltre una disposizione sul monitoraggio e sulla valutazione e una disposizione sull'entrata in vigore e sull'applicabilità del presente regolamento. In particolare, il presente regolamento sostituisce gli articoli da 2 a 6 e il capo 2, sezioni 2 e 3, della decisione 2008/615/GAI del Consiglio e i capi da 2 a 5 e gli articoli 18, 20 e 21 della decisione 2008/616/GAI del Consiglio, che saranno di conseguenza soppressi a decorrere dalla data di applicazione del presente regolamento. L'effetto di tali modifiche sarà che le disposizioni sostituite e soppresse non si applicheranno più a nessuno Stato membro.

²⁷ A seguito delle conclusioni della Commissione nella sua comunicazione del 24 giugno 2020 sulla via da seguire per allineare l'acquis dell'ex terzo pilastro alle norme sulla protezione dei dati (COM(2020) 262 final).

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II"), che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, paragrafo 2, l'articolo 87, paragrafo 2, lettera a), e l'articolo 88, paragrafo 2,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo²⁸,

visto il parere del Comitato delle regioni²⁹,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

- (1) L'Unione si è prefissa l'obiettivo di offrire ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone. Tale obiettivo dovrebbe essere conseguito, tra l'altro, attraverso misure appropriate per prevenire e combattere la criminalità, compresi la criminalità organizzata e il terrorismo.
- (2) Detto obiettivo richiede che le autorità di contrasto si scambino dati in modo efficiente e tempestivo, al fine di combattere efficacemente la criminalità.
- (3) Il presente regolamento ha quindi come obiettivo migliorare, semplificare e facilitare lo scambio di informazioni in materia penale tra le autorità di contrasto degli Stati membri, ma anche con l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) istituita dal regolamento (UE) 2016/794 del Parlamento e del Consiglio³⁰ come polo dell'Unione per lo scambio di informazioni sulla criminalità.
- (4) Le decisioni 2008/615/GAI³¹ e 2008/616/GAI³² del Consiglio, che stabiliscono norme per lo scambio di informazioni tra le autorità competenti per la prevenzione dei reati e le indagini

²⁸GU C del , pag. .

²⁹GU C del , pag. .

³⁰ 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).

³¹ Decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera (GU L 210 del 6.8.2008, pag. 1).

penali, disponendo il trasferimento automatizzato di profili DNA, dati dattiloscopici e determinati dati di immatricolazione dei veicoli, si sono rivelate importanti per combattere il terrorismo e la criminalità transfrontaliera.

- (5) Il presente regolamento dovrebbe definire le condizioni e le procedure per il trasferimento automatizzato di profili DNA, dati dattiloscopici, dati di immatricolazione dei veicoli, immagini del volto ed estratti del casellario giudiziale. Ciò non dovrebbe pregiudicare il trattamento di tali dati nel sistema d'informazione Schengen (SIS), né lo scambio di informazioni supplementari ad essi connesse tramite gli uffici SIRENE, né i diritti delle persone i cui dati sono trattati in tali contesti.
- (6) Il trattamento e lo scambio di dati personali ai fini del presente regolamento non dovrebbero dare luogo ad alcuna forma di discriminazione nei confronti delle persone. Tali attività dovrebbero rispettare pienamente la dignità e l'integrità umana nonché altri diritti fondamentali, compreso il diritto al rispetto della vita privata e alla protezione dei dati personali, conformemente alla Carta dei diritti fondamentali dell'Unione europea.
- (7) Prevedendo la consultazione automatizzata o il confronto automatizzato di profili DNA, dati dattiloscopici, dati di immatricolazione dei veicoli, immagini del volto ed estratti del casellario giudiziale, il presente regolamento mira altresì a consentire la ricerca di persone scomparse e resti umani non identificati. Ciò non dovrebbe pregiudicare l'inserimento nel SIS di segnalazioni di persone scomparse e lo scambio di informazioni supplementari su tali segnalazioni a norma del regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio³³.
- (8) La direttiva (UE) .../... [*sullo scambio di informazioni tra autorità di contrasto degli Stati membri*] fornisce un quadro giuridico coerente dell'Unione per garantire che le autorità di contrasto dispongano di un accesso equivalente alle informazioni in possesso di altri Stati membri quando ne hanno bisogno per combattere la criminalità e il terrorismo. Per intensificare lo scambio di informazioni, tale direttiva formalizza e chiarisce le procedure di condivisione delle informazioni tra gli Stati membri, in particolare a fini di indagine, specificando il ruolo del "punto di contatto unico" e usando appieno il canale di scambio di informazioni di Europol SIENA. Qualsiasi scambio di informazioni che vada al di là di quanto previsto dal presente regolamento dovrebbe essere disciplinato dalla direttiva (UE) .../... [*sullo scambio di informazioni tra autorità di contrasto degli Stati membri*].
- (9) Per la consultazione automatizzata dei dati di immatricolazione dei veicoli, gli Stati membri dovrebbero utilizzare il sistema europeo d'informazione sui veicoli e le patenti di guida (Eucaris) istituito dal trattato relativo a un sistema europeo d'informazione sui veicoli e le patenti di guida (trattato EUCARIS) concepito a tal fine. Eucaris dovrebbe collegare tutti gli Stati membri partecipanti in una rete. Non è necessaria una componente centrale per stabilire la comunicazione, dato che ciascuno Stato membro comunica direttamente con gli altri Stati membri collegati.

³² Decisione 2008/616/GAI del Consiglio, del 23 giugno 2008, relativa all'attuazione della decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera (GU L 210 del 6.8.2008, pag. 12).

³³ Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).

- (10) L'identificazione dell'autore del reato è essenziale per il buon esito delle indagini e delle azioni penali. La consultazione automatizzata delle immagini del volto di indagati e condannati dovrebbe fornire informazioni aggiuntive che permettano di identificare gli autori dei reati e combattere la criminalità.
- (11) La consultazione o il confronto automatizzati di dati biometrici (profili DNA, dati dattiloscopici e immagini del volto) tra le autorità responsabili della prevenzione, dell'accertamento e dell'indagine di reati a norma del presente regolamento dovrebbero riguardare esclusivamente i dati contenuti nelle banche dati istituite a fini di prevenzione, accertamento e indagine di reati.
- (12) La partecipazione allo scambio di estratti del casellario giudiziale dovrebbe rimanere volontaria. Laddove gli Stati membri decidano di partecipare, in uno spirito di reciprocità, non dovrebbe essere loro possibile interrogare le banche dati di altri Stati membri se non mettono a disposizione i propri dati per interrogazioni da parte di altri Stati membri.
- (13) Negli ultimi anni Europol ha ricevuto da vari paesi terzi una grande quantità di dati biometrici di terroristi e criminali, o persone indagate per tali reati. Includere i dati provenienti da paesi terzi conservati presso Europol nel quadro Prüm, e quindi metterli a disposizione delle autorità di contrasto, è necessario per migliorare la prevenzione dei reati e le indagini penali e contribuisce a creare sinergie tra diversi strumenti di contrasto.
- (14) Europol dovrebbe essere in grado di consultare le banche dati degli Stati membri nel contesto del quadro Prüm con i dati ricevuti da paesi terzi al fine di stabilire collegamenti transfrontalieri tra casi di rilevanza penale. La possibilità di utilizzare i dati Prüm, unitamente ad altre banche dati a disposizione di Europol, dovrebbe consentire di effettuare un'analisi più completa e informata delle indagini penali e dovrebbe permettere a Europol di fornire un sostegno migliore alle autorità di contrasto degli Stati membri. In caso di corrispondenza tra i dati utilizzati per la ricerca e quelli conservati nelle banche dati degli Stati membri, questi ultimi possono fornire a Europol le informazioni necessarie allo svolgimento dei suoi compiti.
- (15) Le decisioni 2008/615/GAI e 2008/616/GAI stabiliscono una rete di connessioni bilaterali tra le banche dati nazionali degli Stati membri. Da tale architettura tecnica consegue che ogni Stato membro dovrebbe stabilire almeno 26 connessioni, vale a dire una connessione con ciascuno Stato membro, per ciascuna categoria di dati. Il router e l'indice europeo dei casellari giudiziali (EPRIS) istituiti dal presente regolamento dovrebbero semplificare l'architettura tecnica del quadro Prüm e fungere da punti di connessione tra tutti gli Stati membri. Il router dovrebbe richiedere una connessione unica per Stato membro in relazione ai dati biometrici, mentre EPRIS dovrebbe richiedere una connessione unica per Stato membro in relazione ai casellari giudiziali.
- (16) Il router dovrebbe essere connesso al portale di ricerca europeo istituito dall'articolo 6 del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio³⁴ e dall'articolo 6 del regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio³⁵ al fine di consentire alle

³⁴ Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27).

³⁵ Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85).

autorità degli Stati membri e ad Europol di avviare interrogazioni delle banche dati nazionali a norma del presente regolamento contemporaneamente a interrogazioni dell'archivio comune di dati di identità istituito dall'articolo 17 del regolamento (UE) 2019/817 e dall'articolo 17 del regolamento (UE) 2019/818 a fini di contrasto.

- (17) In caso di corrispondenza tra i dati utilizzati per la ricerca o il confronto e i dati conservati nella banca dati nazionale dello Stato membro o degli Stati membri richiesti, e previa conferma di tale corrispondenza da parte dello Stato membro richiedente, lo Stato membro richiesto dovrebbe trasmettere una serie limitata di dati di base tramite il router entro 24 ore. Il termine dovrebbe garantire uno scambio rapido di comunicazioni tra le autorità degli Stati membri. Gli Stati membri dovrebbero mantenere il controllo della diffusione di tale serie limitata di dati di base. Dovrebbe essere mantenuto un certo grado di intervento umano nei passaggi chiave del processo, anche per quanto riguarda la decisione di trasmettere dati personali allo Stato membro richiedente, al fine di garantire che non siano scambiati in modo automatizzato dati di base.
- (18) Qualsiasi scambio tra le autorità degli Stati membri o con Europol in qualsiasi fase di uno dei processi descritti dal presente regolamento, che non sia esplicitamente descritto in quest'ultimo, dovrebbe avvenire tramite SIENA al fine di garantire che tutti gli Stati membri utilizzino un canale di comunicazione comune, sicuro e affidabile.
- (19) Per lo sviluppo del router e di EPRIS dovrebbe essere utilizzato lo standard del formato universale dei messaggi (UMF). Qualsiasi scambio automatizzato di dati a norma del presente regolamento dovrebbe utilizzare lo standard UMF. Le autorità degli Stati membri ed Europol sono incoraggiate a utilizzare lo standard UMF anche in relazione a ulteriori scambi di dati tra di loro nel quadro Prüm II. Lo standard UMF dovrebbe fungere da standard per lo scambio strutturato delle informazioni a livello transfrontaliero tra i sistemi di informazione, le autorità o le organizzazioni del settore Giustizia e affari interni.
- (20) Solo le informazioni non classificate dovrebbero essere scambiate tramite il quadro Prüm II.
- (21) Taluni aspetti del quadro Prüm II non possono essere trattati in modo esaustivo dal presente regolamento per la loro natura tecnica, fortemente dettagliata e soggetta a frequenti cambiamenti. Tra tali aspetti figurano ad esempio le modalità e le specifiche tecniche per le procedure di consultazione automatizzata, le norme per lo scambio di dati e i dati da scambiare. Al fine di garantire condizioni uniformi di esecuzione del presente regolamento è opportuno attribuire alla Commissione competenze di esecuzione. È opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio³⁶.
- (22) Dato che il presente regolamento prevede l'istituzione del nuovo quadro Prüm, è opportuno sopprimere le disposizioni pertinenti delle decisioni 2008/615/GAI e 2008/616/GAI. È pertanto opportuno modificare di conseguenza tali decisioni.
- (23) Poiché il router dovrebbe essere sviluppato e gestito dall'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), istituita dal regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio³⁷, è

³⁶ 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).

³⁷ Regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia

necessario modificare detto regolamento aggiungendo tale attività ai compiti di eu-LISA. Al fine di consentire la connessione del router al portale di ricerca europeo per poter consultare simultaneamente il router e l'archivio comune di dati di identità, è necessario modificare il regolamento (UE) 2019/817. Al fine di consentire la connessione del router al portale di ricerca europeo per poter consultare simultaneamente il router e l'archivio comune di dati di identità, e per conservare le relazioni e le statistiche del router nell'archivio centrale di relazioni e statistiche, è necessario modificare il regolamento (UE) 2019/818. È pertanto opportuno modificare di conseguenza tali regolamenti.

- (24) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione del presente regolamento, non è da esso vincolata né è soggetta alla sua applicazione.
- (25) [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, l'Irlanda ha notificato che desidera partecipare all'adozione e all'applicazione del presente regolamento.] OPPURE [A norma degli articoli 1 e 2 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda non partecipa all'adozione della presente direttiva, non è da essa vincolata né è soggetta alla sua applicazione.]
- (26) Il Garante europeo della protezione dei dati è stato consultato a norma dell'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio³⁸ e ha espresso un parere in data [XX]³⁹,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO 1

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Il presente regolamento istituisce un quadro per lo scambio di informazioni tra le autorità responsabili della prevenzione, dell'indagine e dell'accertamento di reati (Prüm II).

Il presente regolamento stabilisce le condizioni e le procedure per la consultazione automatizzata di profili DNA, dati dattiloscopici, immagini del volto, estratti del casellario giudiziale e determinati dati di immatricolazione dei veicoli, nonché le norme relative allo scambio di dati di base a seguito di una corrispondenza.

(eu-LISA), che modifica il regolamento (CE) n. 1987/2006 e la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (UE) n. 1077/2011 (GU L 295 del 21.11.2018, pag. 99).

³⁸ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

³⁹ [GU C ... del ..., pag. ...].

Articolo 2

Finalità

Il quadro Prüm II mira a intensificare la cooperazione transfrontaliera nelle materie disciplinate dalla parte III, titolo V, capo 5, del trattato sul funzionamento dell'Unione europea, in particolare lo scambio di informazioni tra autorità responsabili della prevenzione, dell'indagine e dell'accertamento di reati.

Il quadro Prüm II mira altresì a consentire alle autorità responsabili della prevenzione, dell'indagine e dell'accertamento di reati la ricerca di persone scomparse e resti umani non identificati.

Articolo 3

Ambito di applicazione

Il presente regolamento si applica alle banche dati nazionali utilizzate per il trasferimento automatizzato delle categorie di dati seguenti: profili DNA, dati dattiloscopici, immagini del volto, estratti del casellario giudiziale e determinati dati di immatricolazione dei veicoli.

Articolo 4

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

- (1) "loci": la particolare struttura molecolare nelle varie posizioni (loci) del DNA;
- (2) "profilo DNA": un codice alfanumerico che rappresenta una serie di caratteristiche identificative della parte non codificante di un campione di DNA umano analizzato, vale a dire la particolare struttura molecolare nei vari loci del DNA;
- (3) "parte non codificante del DNA": regioni cromosomiche che non contengono alcuna espressione genetica, vale a dire che notoriamente non forniscono alcuna proprietà funzionale di un organismo;
- (4) "dati indicizzati sul DNA": il profilo DNA e il numero di riferimento di cui all'articolo 9;
- (5) "profilo DNA indicizzato": il profilo DNA di una persona identificata;
- (6) "profilo DNA non identificato": il profilo DNA ottenuto da tracce rilevate nel corso delle indagini penali e appartenente a una persona non ancora identificata;
- (7) "dati dattiloscopici": immagini delle impronte digitali, immagini delle impronte digitali latenti, impronte palmari, impronte palmari latenti e modelli di tali immagini (minutiae codificate), quando sono conservati e trattati in una banca dati automatizzata;
- (8) "dati indicizzati dattiloscopici": i dati dattiloscopici e il numero di riferimento di cui all'articolo 14;
- (9) "caso per caso": con riferimento a un singolo fascicolo di indagine;
- (10) "immagine del volto": l'immagine digitalizzata del volto;
- (11) "dati biometrici": profili DNA, dati dattiloscopici o immagini del volto;
- (12) "corrispondenza": la coincidenza risultante da un confronto automatizzato tra dati personali registrati o in fase di registrazione in un sistema di informazione o in una banca dati;
- (13) "candidato": i dati rispetto ai quali è stata verificata una corrispondenza;

- (14) "Stato membro richiedente": lo Stato membro che effettua una consultazione tramite il quadro Prüm II;
- (15) "Stato membro richiesto": lo Stato membro le cui banche dati sono consultate dallo Stato membro richiedente tramite il quadro Prüm II;
- (16) "estratto del casellario giudiziale": qualsiasi informazione disponibile nel registro nazionale o nei registri nazionali che registrano i dati delle autorità competenti a fini di prevenzione, indagine e accertamento di reati;
- (17) "pseudonimizzazione": il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- (18) "dati Europol": qualsiasi dato personale trattato da Europol a norma del regolamento (UE) 2016/794;
- (19) "autorità di controllo": l'autorità pubblica indipendente istituita da uno Stato membro a norma dell'articolo 41 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio⁴⁰;
- (20) "SIENA": l'applicazione di rete per lo scambio sicuro di informazioni, gestita da Europol, volta a facilitare lo scambio di informazioni tra gli Stati membri ed Europol;
- (21) "incidente significativo": qualsiasi incidente, salvo se presenta un impatto limitato ed è probabile che sia già adeguatamente compreso in termini di metodo o tecnologia;
- (22) "minaccia informatica significativa": una minaccia informatica caratterizzata dall'intento, dalla possibilità e dalla capacità di causare un incidente significativo;
- (23) "vulnerabilità significativa": una vulnerabilità che, se sfruttata, porterà probabilmente a un incidente significativo;
- (24) "incidente": un incidente ai sensi dell'articolo 4, paragrafo 5, della direttiva (UE) .../... del Parlamento europeo e del Consiglio⁴¹ [*proposta NIS 2*].

⁴⁰ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

⁴¹ Direttiva (UE) .../... del Parlamento europeo e del Consiglio... (GU...).

CAPO 2
SCAMBIO DI DATI

SEZIONE 1

Profili DNA

Articolo 5

Creazione di schedari nazionali di analisi del DNA

1. Gli Stati membri istituiscono e gestiscono schedari nazionali di analisi del DNA per le indagini penali.

Il trattamento dei dati contenuti negli schedari a norma del presente regolamento è effettuato in conformità del presente regolamento, nel rispetto del diritto nazionale dello Stato membro applicabile al trattamento di tali dati.

2. Gli Stati membri garantiscono che siano disponibili dati indicizzati sul DNA ottenuti dai loro schedari nazionali di analisi del DNA di cui al paragrafo 1.

I dati indicizzati sul DNA non contengono alcun dato che consenta l'identificazione diretta di una persona fisica.

I dati indicizzati sul DNA che non sono attribuiti a nessuno ("profili DNA non identificati") sono riconoscibili come tali.

Articolo 6

Consultazione automatizzata dei profili DNA

1. Gli Stati membri consentono ai punti di contatto nazionali di cui all'articolo 29 e ad Europol di accedere ai dati indicizzati sul DNA presenti nei loro schedari di analisi del DNA per svolgere consultazioni automatizzate confrontando i profili DNA ai fini dell'indagine penale.

Le consultazioni possono essere svolte solo caso per caso e nel rispetto del diritto nazionale dello Stato membro richiedente.

2. Se una consultazione automatizzata rivela che un profilo DNA corrisponde a profili DNA registrati nello schedario consultato dello Stato membro richiesto, il punto di contatto nazionale dello Stato membro richiedente riceve per via automatizzata i dati indicizzati sul DNA con cui è stata riscontrata una corrispondenza.

In caso di mancata corrispondenza, lo Stato membro richiedente ne viene informato per via automatizzata.

3. Il punto di contatto nazionale dello Stato membro richiedente conferma una corrispondenza tra i dati di profili DNA e i dati indicizzati sul DNA conservati dallo Stato membro richiesto a seguito della trasmissione automatizzata dei dati indicizzati sul DNA necessari per confermare la corrispondenza.

Articolo 7

Confronto automatizzato di profili DNA non identificati

1. Tramite i loro punti di contatto nazionali, gli Stati membri possono confrontare i profili DNA dei loro profili DNA non identificati con tutti i profili DNA provenienti da altri schedari nazionali di analisi del DNA ai fini dell'indagine penale. La trasmissione e il confronto dei profili sono effettuati in maniera automatizzata.

2. Se in esito al confronto di cui al paragrafo 1 uno Stato membro richiesto constata una corrispondenza tra profili DNA trasmessi e profili DNA contenuti nei propri schedari di analisi del DNA, comunica senza indugio al punto di contatto nazionale dello Stato membro richiedente i dati indicizzati sul DNA per i quali è stata constatata una corrispondenza.

3. La conferma di una corrispondenza tra i profili DNA e i dati indicizzati sul DNA dello Stato membro richiesto è effettuata dal punto di contatto nazionale dello Stato membro richiedente a seguito della trasmissione automatizzata dei dati indicizzati sul DNA necessari per confermare la corrispondenza.

Articolo 8

Relazioni sugli schedari di analisi del DNA

Ciascuno Stato membro informa la Commissione ed eu-LISA, a norma dell'articolo 73, in merito agli schedari nazionali di analisi del DNA ai quali si applicano gli articoli da 5 a 7.

Articolo 9

Numeri di riferimento per i profili DNA

I numeri di riferimento per i profili DNA sono costituiti da una combinazione degli elementi seguenti:

- (a) un numero di riferimento che consenta agli Stati membri, in caso di corrispondenza, di estrarre ulteriori dati e altre informazioni dalle loro banche dati di cui all'articolo 5 al fine di trasmetterli a uno, ad alcuni o a tutti gli altri Stati membri conformemente agli articoli 47 e 48;
- (b) un codice indicante lo Stato membro che detiene il profilo DNA;
- (c) un codice indicante il tipo di profilo DNA (profili DNA indicizzati o profili DNA non identificati).

Articolo 10

Principi applicati allo scambio di dati indicizzati sul DNA

1. Sono adottate misure appropriate, compresa la cifratura, per garantire la riservatezza e l'integrità dei dati indicizzati sul DNA trasmessi ad altri Stati membri.

2. Gli Stati membri adottano le misure necessarie per garantire l'integrità dei profili DNA messi a disposizione degli altri Stati membri o ad essi inviati per confronto, e per assicurare che tali misure siano conformi alle norme internazionali applicabili allo scambio di dati sul DNA.

3. La Commissione adotta atti di esecuzione per specificare le applicabili norme internazionali che gli Stati membri devono utilizzare per lo scambio di dati indicizzati sul DNA. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 11

Norme per le domande e le risposte concernenti i profili DNA

1. La domanda di consultazione automatizzata o di confronto automatizzato comprende soltanto le informazioni seguenti:

- (a) il codice dello Stato membro richiedente;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) i profili DNA e i relativi numeri di riferimento di cui all'articolo 9;
- (d) i tipi di profili DNA trasmessi (profili DNA non identificati o profili DNA indicizzati).

2. La risposta alla domanda di cui al paragrafo 1 contiene soltanto le informazioni seguenti:

- (a) l'indicazione della presenza di una o più corrispondenze, o della mancanza di corrispondenze;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) la data, l'ora e il numero di riferimento della risposta;
- (d) i codici dello Stato membro richiedente e dello Stato membro richiesto;
- (e) i numeri di riferimento dei profili DNA dello Stato membro richiedente e dello Stato membro richiesto;
- (f) i tipi di profili DNA trasmessi (profili DNA non identificati o profili DNA indicizzati);
- (g) i profili DNA per i quali è stata riscontrata una corrispondenza.

3. La notifica automatizzata di una corrispondenza è fornita soltanto se la consultazione o il confronto automatizzati abbiano evidenziato una corrispondenza di un numero minimo di loci. La Commissione adotta atti di esecuzione per specificare tale numero minimo di loci secondo la procedura di cui all'articolo 76, paragrafo 2.

4. Se una consultazione o un confronto con profili DNA non identificati produce una corrispondenza, ciascuno Stato membro richiesto che disponga di dati corrispondenti può inserire nella propria banca dati nazionale un contrassegno indicante che è stata riscontrata una corrispondenza per tale profilo DNA a seguito della consultazione o del confronto effettuato da un altro Stato membro.

5. Gli Stati membri provvedono affinché le domande siano coerenti con le dichiarazioni inviate a norma dell'articolo 8. Tali dichiarazioni figurano nel manuale pratico di cui all'articolo 78.

SEZIONE 2

Dati dattiloscopici

Articolo 12

Dati indicizzati dattiloscopici

1. Gli Stati membri garantiscono che siano disponibili dati indicizzati dattiloscopici ottenuti dai sistemi nazionali automatizzati di identificazione dattiloscopica istituiti per la prevenzione, l'indagine e l'accertamento di reati.

2. I dati indicizzati dattiloscopici non contengono alcun dato che consenta l'identificazione diretta di una persona fisica.

3. I dati indicizzati dattiloscopici che non sono attribuiti a nessuna persona fisica ("dati dattiloscopici non identificati") sono riconoscibili come tali.

Articolo 13

Consultazione automatizzata di dati dattiloscopici

1. Ai fini della prevenzione, dell'indagine e dell'accertamento di reati, gli Stati membri autorizzano i punti di contatto nazionali degli altri Stati membri ed Europol ad accedere ai dati indicizzati dattiloscopici dei loro sistemi automatizzati di identificazione dattiloscopica creati a tal fine, per procedere a consultazioni automatizzate tramite il confronto dei dati indicizzati dattiloscopici.

Le consultazioni possono essere svolte solo caso per caso e nel rispetto del diritto nazionale dello Stato membro richiedente.

2. Il punto di contatto nazionale dello Stato membro richiedente conferma una corrispondenza tra i dati dattiloscopici e i dati indicizzati dattiloscopici conservati dallo Stato membro richiesto a seguito della trasmissione automatizzata dei dati indicizzati dattiloscopici necessari per confermare la corrispondenza.

Articolo 14

Numeri di riferimento per i dati dattiloscopici

I numeri di riferimento per i dati dattiloscopici sono costituiti da una combinazione degli elementi seguenti:

- (a) un numero di riferimento che consenta agli Stati membri, in caso di corrispondenza, di estrarre dati ulteriori e altre informazioni dalle loro banche dati di cui all'articolo 12 al fine di trasmetterli a uno, ad alcuni o a tutti gli Stati membri conformemente agli articoli 47 e 48;
- (b) un codice indicante lo Stato membro che detiene i dati dattiloscopici.

Articolo 15

Principi applicati allo scambio di dati dattiloscopici

1. La digitalizzazione dei dati dattiloscopici e la loro trasmissione agli altri Stati membri è effettuata secondo un formato dati uniforme. La Commissione adotta atti di esecuzione per specificare tale formato dati uniforme secondo la procedura di cui all'articolo 76, paragrafo 2.

2. Ciascuno Stato membro garantisce che i dati dattiloscopici da esso trasmessi siano di qualità sufficiente per un confronto tramite i sistemi automatizzati di identificazione dattiloscopica.

3. Gli Stati membri adottano misure appropriate, compresa la cifratura, per garantire la riservatezza e l'integrità dei dati dattiloscopici trasmessi agli altri Stati membri.

4. La Commissione adotta atti di esecuzione per specificare le norme esistenti applicabili allo scambio di dati dattiloscopici che devono essere utilizzate dagli Stati membri. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 16

Capacità di consultazione per i dati dattiloscopici

1. Ogni Stato membro provvede affinché le sue domande di consultazione non eccedano le capacità di consultazione specificate dallo Stato membro richiesto.

Gli Stati membri informano la Commissione ed eu-LISA, conformemente all'articolo 79, paragrafi 8 e 10, in merito alle loro capacità massime di consultazione giornaliera per i dati dattiloscopici di persone identificate e per i dati dattiloscopici di persone non ancora identificate.

2. La Commissione adotta atti di esecuzione per specificare il numero massimo di candidati accettati ai fini del confronto per ciascuna trasmissione, secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 17

Norme sulle domande e sulle risposte concernenti i dati dattiloscopici

1. Una domanda di consultazione automatizzata comprende soltanto le informazioni seguenti:

- (a) il codice dello Stato membro richiedente;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) i dati dattiloscopici e i relativi numeri di riferimento di cui all'articolo 14.

2. La risposta alla domanda di cui al paragrafo 1 contiene soltanto le informazioni seguenti:

- (a) l'indicazione della presenza di una o più corrispondenze, o della mancanza di corrispondenze;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) la data, l'ora e il numero di riferimento della risposta;
- (d) i codici dello Stato membro richiedente e dello Stato membro richiesto;
- (e) i numeri di riferimento dei dati dattiloscopici dello Stato membro richiedente e dello Stato membro richiesto;
- (f) i dati dattiloscopici per i quali è stata riscontrata una corrispondenza.

SEZIONE 3

Dati di immatricolazione dei veicoli

Articolo 18

Consultazione automatizzata di dati di immatricolazione dei veicoli

1. Ai fini della prevenzione, dell'indagine e dell'accertamento di reati, gli Stati membri consentono ai punti di contatto nazionali di altri Stati membri ed a Europol l'accesso ai seguenti dati nazionali di immatricolazione dei veicoli, per condurre consultazioni automatizzate caso per caso:

- (a) dati relativi ai proprietari o agli utenti;
- (b) dati relativi ai veicoli.

2. Le consultazioni possono essere effettuate soltanto con un numero completo di telaio o un numero completo di immatricolazione.

3. Le consultazioni possono essere svolte solo nel rispetto del diritto nazionale dello Stato membro richiedente.

Articolo 19

Principi applicati alla consultazione automatizzata di dati di immatricolazione dei veicoli

1. Per la consultazione automatizzata di dati di immatricolazione dei veicoli, gli Stati membri utilizzano il sistema europeo d'informazione sui veicoli e le patenti di guida (Eucaris).
2. Le informazioni scambiate tramite Eucaris sono trasmesse in forma cifrata.
3. La Commissione adotta atti di esecuzione per specificare i dati di immatricolazione dei veicoli da scambiare. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 20

Registrazioni

1. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dal personale delle proprie autorità debitamente autorizzato a scambiare dati di immatricolazione dei veicoli, nonché le registrazioni delle interrogazioni richieste da altri Stati membri. Europol conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato.

Ciascuno Stato membro ed Europol conservano le registrazioni di tutti i trattamenti di dati riguardanti i dati di immatricolazione dei veicoli. Tali registrazioni comprendono gli elementi seguenti:

- (a) lo Stato membro o l'agenzia dell'Unione che ha avviato la domanda di interrogazione;
- (b) la data e l'ora della domanda;
- (c) la data e l'ora della risposta;
- (d) le banche dati nazionali a cui è stata inviata la domanda di interrogazione;
- (e) le banche dati nazionali che hanno fornito una risposta positiva.

2. Le registrazioni di cui al paragrafo 1 possono essere utilizzate unicamente per la raccolta di statistiche e per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi.

Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Qualora, tuttavia, siano necessarie per procedure di monitoraggio già avviate, sono cancellate quando le procedure di monitoraggio non necessitano più delle registrazioni.

3. Per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, i titolari del trattamento hanno accesso alle registrazioni per la verifica interna di cui all'articolo 56.

SEZIONE 4

Immagini del volto

Articolo 21

Immagini del volto

1. Gli Stati membri garantiscono che siano disponibili immagini del volto ottenute dalle loro banche dati nazionali istituite per la prevenzione, l'indagine e l'accertamento di reati. Tali dati comprendono

soltanto immagini del volto e il numero di riferimento di cui all'articolo 23 e indicano se le immagini del volto sono attribuite o meno a una persona.

Gli Stati membri non mettono a disposizione in tale contesto dati dai quali sia possibile identificare direttamente una persona.

2. Le immagini del volto non attribuite a una persona (immagini del volto non identificate) sono riconoscibili come tali.

Articolo 22

Consultazione automatizzata di immagini del volto

1. Ai fini della prevenzione, dell'indagine e dell'accertamento di reati, gli Stati membri consentono ai punti di contatto nazionali di altri Stati membri e ad Europol di accedere alle immagini del volto conservate nelle loro banche dati nazionali per condurre consultazioni automatizzate.

Le consultazioni possono essere svolte solo caso per caso e nel rispetto del diritto nazionale dello Stato membro richiedente.

2. Lo Stato membro richiedente riceve un elenco di corrispondenze relative a possibili candidati. Tale Stato membro esamina l'elenco per stabilire l'esistenza di una corrispondenza confermata.

3. È stabilita una norma minima di qualità per consentire la consultazione e il confronto delle immagini del volto. La Commissione adotta atti di esecuzione per specificare tale norma minima di qualità. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 23

Numeri di riferimento per le immagini del volto

I numeri di riferimento per le immagini del volto sono costituiti dalla combinazione degli elementi seguenti:

- (a) un numero di riferimento che consenta agli Stati membri, in caso di corrispondenza, di estrarre ulteriori dati e altre informazioni dalle loro banche dati di cui all'articolo 21 al fine di trasmetterli a uno, ad alcuni o a tutti gli altri Stati membri conformemente agli articoli 47 e 48;
- (b) un codice indicante lo Stato membro che detiene le immagini del volto.

Articolo 24

Norme sulle domande e sulle risposte concernenti le immagini del volto

1. Una domanda di consultazione automatizzata comprende soltanto le informazioni seguenti:

- (a) il codice dello Stato membro richiedente;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) le immagini del volto e i relativi numeri di riferimento di cui all'articolo 23.

2. La risposta alla domanda di cui al paragrafo 1 contiene soltanto le informazioni seguenti:

- (a) l'indicazione della presenza di una o più corrispondenze, o della mancanza di corrispondenze;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) la data, l'ora e il numero di riferimento della risposta;

- (d) i codici dello Stato membro richiedente e dello Stato membro richiesto;
- (e) i numeri di riferimento delle immagini del volto dello Stato membro richiedente e dello Stato membro richiesto;
- (f) le immagini del volto per le quali è stata riscontrata una corrispondenza.

SEZIONE 5

Estratti del casellario giudiziale

Articolo 25

Estratti del casellario giudiziale

1. Gli Stati membri possono decidere di partecipare allo scambio automatizzato di estratti del casellario giudiziale. Gli Stati membri che partecipano allo scambio automatizzato di estratti del casellario giudiziale garantiscono la disponibilità dei dati anagrafici di indagati e criminali desunti dai rispettivi indici dei casellari giudiziali nazionali istituiti ai fini delle indagini penali. Tale serie di dati, se disponibile, contiene i dati seguenti:

- (a) nome/i;
- (b) cognome/i;
- (c) alias;
- (d) data di nascita;
- (e) cittadinanza o cittadinanze;
- (f) luogo e paese di nascita;
- (g) sesso.

2. I dati di cui al paragrafo 1, lettere a), b), c), e) ed f), sono pseudonimizzati.

Articolo 26

Consultazione automatizzata di estratti del casellario giudiziale

1. Ai fini delle indagini penali, gli Stati membri consentono ai punti di contatto nazionali degli altri Stati membri e ad Europol di accedere ai dati dei rispettivi indici dei casellari giudiziali nazionali per effettuare consultazioni automatizzate.

Le consultazioni possono essere svolte solo caso per caso e nel rispetto del diritto nazionale dello Stato membro richiedente.

2. Lo Stato membro richiedente riceve l'elenco delle corrispondenze con indicazione della relativa qualità.

Lo Stato membro richiedente viene altresì informato in merito allo Stato membro la cui banca dati contiene i dati che hanno determinato la corrispondenza in questione.

Articolo 27

Numeri di riferimento per gli estratti del casellario giudiziale

I numeri di riferimento per gli estratti del casellario giudiziale sono costituiti dalla combinazione degli elementi seguenti:

- (a) un numero di riferimento che consenta agli Stati membri, in caso di corrispondenza, di estrarre dati personali e altre informazioni dai loro indici di cui all'articolo 25 al fine di trasmetterli a uno, ad alcuni o a tutti gli Stati membri conformemente agli articoli 47 e 48;
- (b) un codice indicante lo Stato membro che detiene l'estratto del casellario giudiziale.

Articolo 28

Norme sulle domande e sulle risposte concernenti gli estratti del casellario giudiziale

1. Una domanda di consultazione automatizzata comprende soltanto le informazioni seguenti:

- (a) il codice dello Stato membro richiedente;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) gli estratti del casellario giudiziale e i relativi numeri di riferimento di cui all'articolo 27.

2. La risposta alla domanda di cui al paragrafo 1 contiene soltanto le informazioni seguenti:

- (a) l'indicazione della presenza di una o più corrispondenze, o della mancanza di corrispondenze;
- (b) la data, l'ora e il numero di riferimento della domanda;
- (c) la data, l'ora e il numero di riferimento della risposta;
- (d) i codici dello Stato membro richiedente e dello Stato membro richiesto;
- (e) i numeri di riferimento degli estratti del casellario giudiziale dello Stato membro richiedente e dello Stato membro richiesto.

SEZIONE 6

Disposizioni comuni

Articolo 29

Punti di contatto nazionali

Ciascuno Stato membro designa un punto di contatto nazionale.

I punti di contatto nazionali sono competenti per la fornitura dei dati di cui agli articoli 6, 7, 13, 18, 22 e 26.

Articolo 30

Misure di attuazione

La Commissione adotta atti di esecuzione per specificare le modalità tecniche delle procedure di cui agli articoli 6, 7, 13, 18, 22 e 26. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 31

Specifiche tecniche

Gli Stati membri ed Europol osservano specifiche tecniche comuni per quanto riguarda tutte le domande e le risposte relative alle consultazioni e ai confronti dei profili DNA, dei dati dattiloscopici, dei dati di immatricolazione dei veicoli, delle immagini del volto e degli estratti del casellario giudiziale. La Commissione adotta atti di esecuzione per specificare tali specifiche tecniche secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 32

Disponibilità dello scambio automatizzato di dati a livello nazionale

1. Gli Stati membri adottano tutte le misure necessarie per garantire che la consultazione automatizzata o il confronto automatizzato di profili DNA, dati dattiloscopici, dati di immatricolazione dei veicoli, immagini del volto ed estratti del casellario giudiziale possa effettuarsi 24 ore su 24 e 7 giorni su 7.
2. I punti di contatto nazionali provvedono immediatamente a informarsi reciprocamente e a informare la Commissione, Europol ed eu-LISA in merito a un guasto tecnico che causi l'indisponibilità dello scambio automatizzato di dati.

I punti di contatto nazionali concordano a titolo temporaneo sistemi alternativi di scambio di informazioni conformemente al diritto dell'Unione e alla normativa nazionale applicabili.

3. I punti di contatto nazionali ristabiliscono senza indugio lo scambio automatizzato di dati.

Articolo 33

Giustificazione per il trattamento dei dati

1. Ciascuno Stato membro conserva una giustificazione delle interrogazioni formulate dalle sue autorità competenti.

Europol conserva una giustificazione delle interrogazioni che formula.

2. La giustificazione di cui al paragrafo 1 contiene:

- (a) la finalità dell'interrogazione, compreso un riferimento al caso specifico o all'indagine specifica;
- (b) l'indicazione dell'eventualità che l'interrogazione riguardi un indagato o l'autore di un reato;
- (c) l'indicazione dell'eventualità che l'interrogazione intenda identificare uno sconosciuto od ottenere maggiori dati su una persona nota.

3. Le giustificazioni di cui al paragrafo 2 sono utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità dell'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi.

Le giustificazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Qualora, tuttavia, siano necessarie per procedure di monitoraggio già avviate, sono cancellate quando le procedure di monitoraggio non necessitano più di giustificazione.

4. Per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, i titolari del trattamento hanno accesso a tali giustificazioni per la verifica interna di cui all'articolo 56.

Articolo 34

Uso del formato universale dei messaggi

1. Per lo sviluppo del router di cui all'articolo 35 e di EPRIS è utilizzato lo standard del formato universale dei messaggi (UMF).
2. Qualsiasi scambio automatizzato di dati a norma del presente regolamento utilizza lo standard UMF.

CAPO 3

ARCHITETTURA

SEZIONE 1

Router

Articolo 35

Router

1. Viene istituito un router al fine di facilitare l'instaurazione di connessioni tra gli Stati membri e con Europol per l'interrogazione e l'estrazione dei dati biometrici e l'assegnazione di un punteggio alle relative corrispondenze in conformità del presente regolamento.
2. Il router è costituito da:
 - (a) un'infrastruttura centrale, che comprende uno strumento di ricerca per l'interrogazione simultanea delle banche dati degli Stati membri di cui agli articoli 5, 12 e 21, nonché dei dati Europol;
 - (b) un canale di comunicazione sicuro tra l'infrastruttura centrale e gli Stati membri e le agenzie dell'Unione autorizzate a usare il router;
 - (c) un'infrastruttura di comunicazione sicura tra l'infrastruttura centrale e il portale di ricerca europeo ai fini dell'articolo 39.

Articolo 36

Uso del router

L'uso del router è riservato alle autorità degli Stati membri che hanno accesso allo scambio di profili DNA, dati dattiloscopici e immagini del volto, nonché a Europol, a norma del presente regolamento e del regolamento (UE) 2016/794.

Articolo 37

Interrogazioni

1. Gli utenti del router di cui all'articolo 36 presentano una domanda di interrogazione trasmettendo dati biometrici al router. Il router invia la domanda di interrogazione alle banche dati degli Stati membri e ai dati Europol simultaneamente ai dati presentati dall'utente e conformemente ai suoi diritti di accesso.
2. Quando riceve una domanda di interrogazione dal router, ciascuno Stato membro richiesto ed Europol interrogano le proprie banche dati in modo automatizzato e senza indugio.

3. Eventuali corrispondenze risultanti dall'interrogazione delle banche dati di ciascuno Stato membro e dei dati Europol sono rinviate al router in modo automatizzato.
4. Il router classifica le risposte in base al punteggio della corrispondenza tra i dati biometrici utilizzati per l'interrogazione e i dati biometrici conservati nelle banche dati degli Stati membri e nei dati Europol.
5. Il router rinvia all'utente l'elenco dei dati biometrici per i quali è stata riscontrata una corrispondenza e i relativi punteggi.
6. La Commissione adotta atti di esecuzione per specificare la procedura tecnica utilizzata dal router per interrogare le banche dati degli Stati membri e i dati Europol, il formato delle risposte del router, nonché le norme tecniche per l'assegnazione di punteggi alla corrispondenza tra dati biometrici. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 38

Controllo della qualità

Lo Stato membro richiesto verifica senza indugio la qualità dei dati trasmessi con una procedura interamente automatizzata.

Qualora i dati risultino non idonei per un confronto automatizzato, lo Stato membro richiesto ne informa senza indugio lo Stato membro richiedente tramite il router.

Articolo 39

Interoperabilità tra il router e l'archivio comune di dati di identità ai fini dell'accesso da parte delle autorità di contrasto

1. Gli utenti del router di cui all'articolo 36 possono avviare un'interrogazione delle banche dati degli Stati membri e dei dati Europol simultaneamente a un'interrogazione dell'archivio comune di dati di identità se sono soddisfatte le condizioni pertinenti ai sensi del diritto dell'Unione e conformemente ai loro diritti di accesso. A tal fine il router interroga l'archivio comune di dati di identità tramite il portale di ricerca europeo.
2. Le interrogazioni rivolte all'archivio comune di dati di identità per fini di contrasto sono effettuate conformemente all'articolo 22 del regolamento (UE) 2019/817 e all'articolo 22 del regolamento (UE) 2019/818. Qualsiasi risultato derivante dalle interrogazioni viene trasmesso tramite il portale di ricerca europeo.

Soltanto le autorità designate ai sensi dell'articolo 4, punto 20, del regolamento (UE) 2019/817 e dell'articolo 4, punto 20, del regolamento (UE) 2019/818 possono avviare tali interrogazioni simultanee.

Le interrogazioni simultanee delle banche dati degli Stati membri, dei dati Europol e dell'archivio comune di dati di identità possono essere avviate soltanto nei casi in cui è probabile che i dati relativi a un indagato, all'autore di un reato o a una vittima di un reato di terrorismo o di altri reati gravi quali definiti rispettivamente all'articolo 4, punti 21 e 22, del regolamento (UE) 2019/817 e all'articolo 4, punti 21 e 22, del regolamento (UE) 2019/818, siano conservati nell'archivio comune di dati di identità.

Articolo 40

Registrazioni

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

- (a) lo Stato membro o l'agenzia dell'Unione che ha avviato la domanda di interrogazione;
- (b) la data e l'ora della domanda;
- (c) la data e l'ora della risposta;
- (d) le banche dati nazionali o i dati Europol a cui è stata inviata la domanda di interrogazione;
- (e) le banche dati nazionali o i dati Europol che hanno fornito una risposta;
- (f) ove applicabile, il fatto che è stata effettuata un'interrogazione simultanea dell'archivio comune di dati di identità.

2. Ciascuno Stato membro conserva le registrazioni delle interrogazioni effettuate dalle proprie autorità competenti e dal personale di tali autorità debitamente autorizzato a usare il router, nonché le registrazioni delle interrogazioni richieste da altri Stati membri.

Europol conserva le registrazioni delle interrogazioni effettuate dal proprio personale debitamente autorizzato.

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per la raccolta di statistiche e per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, e per garantire l'integrità e la sicurezza degli stessi.

Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione. Qualora, tuttavia, siano necessarie per procedure di monitoraggio già avviate, sono cancellate quando le procedure di monitoraggio non necessitano più delle registrazioni.

4. Per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, i titolari del trattamento hanno accesso alle registrazioni per la verifica interna di cui all'articolo 56.

Articolo 41

Procedure di notifica in caso di impossibilità tecnica dell'uso del router

1. Qualora sia tecnicamente impossibile utilizzare il router per interrogare una o più banche dati nazionali o dati Europol a causa di un guasto del router, eu-LISA ne informa gli utenti in modo automatizzato. eu-LISA adotta misure per far fronte senza indugio all'impossibilità tecnica di utilizzare il router.

2. Qualora sia tecnicamente impossibile usare il router per interrogare una o più banche dati nazionali o i dati Europol a causa di un guasto dell'infrastruttura nazionale di uno Stato membro, quest'ultimo ne informa gli altri Stati membri, eu-LISA e la Commissione in modo automatizzato. Gli Stati membri adottano misure per affrontare senza indugio l'impossibilità tecnica di utilizzare il router.

3. Qualora sia tecnicamente impossibile usare il router per interrogare una o più banche dati nazionali o i dati Europol a causa di un guasto dell'infrastruttura di Europol, Europol ne informa gli Stati membri, eu-LISA e la Commissione in modo automatizzato. Europol adotta misure per affrontare senza indugio l'impossibilità tecnica di utilizzare il router.

SEZIONE 2

EPRIS

Articolo 42

EPRIS

1. Per la consultazione automatizzata degli estratti del casellario giudiziale di cui all'articolo 26, gli Stati membri ed Europol utilizzano l'indice europeo dei casellari giudiziali (EPRIS).

2. EPRIS è costituito da:

- (a) un'infrastruttura centrale, comprendente uno strumento di consultazione che consenta l'interrogazione simultanea delle banche dati degli Stati membri;
- (b) un canale di comunicazione sicuro tra l'infrastruttura centrale di EPRIS, gli Stati membri ed Europol.

Articolo 43

Uso di EPRIS

1. Ai fini della consultazione degli estratti del casellario giudiziale tramite EPRIS, è necessario utilizzare la serie di dati seguente:

- (a) nome/i;
- (b) cognome/i;
- (c) data di nascita.

2. Laddove disponibile si può utilizzare anche la serie di dati seguente:

- (a) alias;
- (b) cittadinanza o cittadinanze;
- (c) luogo e paese di nascita;
- (d) sesso.

3. I dati di cui al paragrafo 1, lettere a) e b), e al paragrafo 2, lettere a), b) e c), utilizzati per le interrogazioni sono pseudonimizzati.

Articolo 44

Interrogazioni

1. Gli Stati membri ed Europol presentano una domanda di interrogazione fornendo i dati di cui all'articolo 43.

EPRIS invia la domanda di interrogazione alle banche dati degli Stati membri con i dati presentati dallo Stato membro richiedente e conformemente al presente regolamento.

2. Quando riceve una domanda di interrogazione da EPRIS, ciascuno Stato membro interroga l'indice dei casellari giudiziali nazionale in modo automatizzato e senza indugio.

3. Eventuali corrispondenze risultanti dall'interrogazione della banca dati di ciascuno Stato membro sono rinviate ad EPRIS in modo automatizzato.

4. L'elenco delle corrispondenze è rinviato da EPRIS allo Stato membro richiedente. L'elenco delle corrispondenze indica la qualità della corrispondenza nonché lo Stato membro la cui banca dati contiene i dati che hanno determinato la corrispondenza.

5. Quando riceve l'elenco delle corrispondenze, lo Stato membro richiedente decide quali sono le corrispondenze alle quali è necessario dare seguito e invia una domanda motivata di follow-up contenente qualsiasi ulteriore informazione pertinente allo Stato membro o agli Stati membri richiesti tramite SIENA.

6. Lo Stato membro o gli Stati membri richiesti trattano tali domande senza indugio per decidere se condividere i dati conservati nella loro banca dati.

In seguito a conferma, lo Stato membro o gli Stati membri richiesti condividono i dati di cui all'articolo 43, se disponibili. Lo scambio di informazioni ha luogo tramite SIENA.

7. La Commissione adotta atti di esecuzione per specificare la procedura tecnica di interrogazione da parte di EPRIS delle banche dati degli Stati membri e il formato delle risposte. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

Articolo 45

Registrazioni

1. Europol conserva le registrazioni di tutti i trattamenti di dati in EPRIS. Tali registrazioni comprendono gli elementi seguenti:

- (a) lo Stato membro o l'agenzia dell'Unione che ha avviato la domanda di interrogazione;
- (b) la data e l'ora della domanda;
- (c) la data e l'ora della risposta;
- (d) le banche dati nazionali a cui è stata inviata la domanda di interrogazione;
- (e) le banche dati nazionali che hanno fornito una risposta.

2. Ciascuno Stato membro conserva le registrazioni delle domande di interrogazione effettuate dalle proprie autorità competenti e dal personale di tali autorità debitamente autorizzato a usare EPRIS. Europol conserva le registrazioni delle domande di interrogazione effettuate dal proprio personale debitamente autorizzato.

3. Le registrazioni di cui ai paragrafi 1 e 2 possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, e per garantire la sicurezza e l'integrità degli stessi.

Le registrazioni sono protette dall'accesso non autorizzato con misure adeguate e sono cancellate un anno dopo la loro creazione.

Qualora, tuttavia, siano necessarie per procedure di monitoraggio già avviate, sono cancellate quando le procedure di monitoraggio non necessitano più delle registrazioni.

4. Per il monitoraggio ai fini della protezione dei dati, compresa la verifica dell'ammissibilità di un'interrogazione e della liceità del trattamento dei dati, i titolari del trattamento hanno accesso alle registrazioni per la verifica interna di cui all'articolo 56.

Articolo 46

Procedure di notifica in caso di impossibilità tecnica dell'uso di EPRIS

1. Qualora sia tecnicamente impossibile usare EPRIS per interrogare una o più banche dati nazionali a causa di un guasto dell'infrastruttura di Europol, quest'ultima ne informa gli Stati membri in modo automatizzato. Europol adotta misure per affrontare senza indugio l'impossibilità tecnica di utilizzare EPRIS.
2. Qualora sia tecnicamente impossibile usare EPRIS per interrogare una o più banche dati nazionali a causa di un guasto dell'infrastruttura nazionale di uno Stato membro, quest'ultimo ne informa Europol e la Commissione in modo automatizzato. Gli Stati membri adottano misure per affrontare senza indugio l'impossibilità tecnica di utilizzare EPRIS.

CAPO 4

SCAMBIO DI DATI A SEGUITO DI UNA CORRISPONDENZA

Articolo 47

Scambio di dati di base

Se le procedure di cui agli articoli 6, 7, 13 o 22 mostrano una corrispondenza tra i dati utilizzati per la consultazione o il confronto e i dati conservati nella banca dati dello Stato membro o degli Stati membri richiesti, e previa conferma di tale corrispondenza da parte dello Stato membro richiedente, lo Stato membro richiesto rinvia entro 24 ore una serie di dati di base tramite il router. Tale insieme di dati di base, se disponibile, contiene i dati seguenti:

- (a) nome/i;
- (b) cognome/i;
- (c) data di nascita;
- (d) cittadinanza o cittadinanze;
- (e) luogo e paese di nascita;
- (f) sesso.

Articolo 48

Uso di SIENA

Qualsiasi scambio non espressamente previsto dal presente regolamento tra le autorità competenti degli Stati membri o con Europol, in qualsiasi fase di ognuna delle procedure previste dal presente regolamento, avviene tramite SIENA.

CAPO 5
EUROPOL

Articolo 49

Accesso da parte degli Stati membri ai dati biometrici provenienti da paesi terzi conservati da Europol

1. A norma del regolamento (UE) 2016/794, gli Stati membri hanno accesso tramite il router ai dati biometrici forniti a Europol da paesi terzi per le finalità di cui all'articolo 18, paragrafo 2, lettere a), b) e c), del medesimo regolamento, e possono consultare tali dati tramite il router.
2. Qualora emerga una corrispondenza tra i dati utilizzati per la consultazione e i dati Europol, è dato seguito alla procedura conformemente al regolamento (UE) 2016/794.

Articolo 50

Accesso da parte di Europol ai dati conservati nelle banche dati degli Stati membri

1. A norma del regolamento (UE) 2016/794, Europol ha accesso ai dati conservati dagli Stati membri nelle banche dati nazionali conformemente al presente regolamento.
2. Le interrogazioni di Europol effettuate usando i dati biometrici come criterio di ricerca sono svolte tramite il router.
3. Le interrogazioni di Europol effettuate usando i dati di immatricolazione dei veicoli come criterio di ricerca sono svolte tramite Eucaris.
4. Le interrogazioni di Europol effettuate usando i casellari giudiziari come criterio di ricerca sono svolte utilizzando EPRIS.
5. Europol effettua le consultazioni a norma del paragrafo 1 soltanto nell'espletamento dei suoi compiti di cui al regolamento (UE) 2016/794.
6. Se le procedure di cui agli articoli 6, 7, 13 o 22 mostrano una corrispondenza tra i dati utilizzati per la consultazione o il confronto e i dati conservati nella banca dati nazionale dello Stato membro o degli Stati membri richiesti, e previa conferma di tale corrispondenza da parte di Europol, lo Stato membro richiesto decide entro 24 ore se rinviare una serie di dati di base tramite il router. Tale insieme di dati di base, se disponibile, contiene i dati seguenti:
 - (a) nome/i;
 - (b) cognome/i;
 - (c) data di nascita;
 - (d) cittadinanza o cittadinanze;
 - (e) luogo e paese di nascita;
 - (f) sesso.
7. L'utilizzo da parte di Europol delle informazioni ottenute da una consultazione effettuata a norma del paragrafo 1 e dallo scambio di dati fondamentali a norma del paragrafo 6 è soggetto al consenso dello Stato membro nella cui banca dati è stata riscontrata la corrispondenza. Se lo Stato membro acconsente all'uso di tali informazioni, il loro trattamento da parte di Europol è disciplinato dal regolamento (UE) 2016/794.

CAPO 6
PROTEZIONE DEI DATI

Articolo 51

Finalità dei dati

1. Lo Stato membro richiedente o Europol può trattare i dati personali solamente ai fini per i quali i dati sono stati trasmessi dallo Stato membro richiesto a norma del presente regolamento. Il trattamento per altri fini è consentito esclusivamente previa autorizzazione dello Stato membro richiesto.
2. Il trattamento dei dati trasmessi a norma degli articoli 6, 7, 13, 18 o 22, da parte dello Stato membro che effettua la consultazione o il confronto è autorizzato esclusivamente allo scopo di:
 - (a) stabilire se esista una corrispondenza tra i profili DNA, i dati dattiloscopici, i dati di immatricolazione dei veicoli, le immagini del volto e gli estratti del casellario giudiziale oggetto del confronto;
 - (b) predisporre e introdurre una domanda di assistenza giudiziaria da parte delle autorità di polizia in caso di corrispondenza tra i dati;
 - (c) conservare registrazioni a norma degli articoli 40 e 45.
3. Lo Stato membro richiedente può trattare i dati fornitigli a norma degli articoli 6, 7, 13 o 22 solo se necessario ai fini del presente regolamento. Al termine del confronto o della risposta automatizzata alle consultazioni, i dati trasmessi sono immediatamente cancellati a meno che non sia necessario un ulteriore trattamento da parte dello Stato membro richiedente a fini di prevenzione, indagine e accertamento di reati.
4. I dati forniti a norma dell'articolo 18 possono essere utilizzati dallo Stato membro richiedente solo se necessario ai fini del presente regolamento. Al termine della risposta automatizzata alle consultazioni, i dati trasmessi sono immediatamente cancellati a meno che non sia necessario un ulteriore trattamento per la registrazione a norma dell'articolo 20. Lo Stato membro richiedente utilizza i dati ricevuti in una risposta esclusivamente ai fini della procedura in base alla quale è stata effettuata la consultazione.

Articolo 52

Esattezza, pertinenza e conservazione dei dati

1. Gli Stati assicurano l'esattezza e l'attualità dei dati personali. Qualora uno Stato membro richiesto venga a conoscenza del fatto che sono stati forniti dati inesatti o dati che non avrebbero dovuto essere stati trasmessi, ogni Stato membro richiedente ne è informato quanto prima. Tutti gli Stati membri richiedenti interessati sono tenuti a rettificare o cancellare i dati di conseguenza. I dati personali trasmessi sono rettificati se risultano inesatti. Lo Stato membro richiedente che ha motivo di ritenere che i dati trasmessi siano inesatti o che debbano essere cancellati ne informa immediatamente lo Stato membro richiesto.
2. Qualora l'interessato contesti l'esattezza dei dati in possesso di uno Stato membro, qualora lo Stato membro non sia in grado di accertarne l'esattezza in modo attendibile e qualora ciò sia richiesto dall'interessato, i dati in questione sono contrassegnati da un indicatore di validità ("flag"). Nei casi in cui è apposto l'indicatore di validità, gli Stati membri possono toglierlo solo con il consenso dell'interessato o su decisione dell'organo giurisdizionale competente o dell'autorità indipendente di protezione dei dati.

3. I dati forniti che non avrebbero dovuto essere trasmessi o ricevuti sono cancellati. I dati lecitamente trasmessi e ricevuti sono cancellati:

- (a) se non sono o non sono più necessari per le finalità per le quali sono stati trasmessi;
- (b) al termine del periodo massimo di conservazione dei dati a norma del diritto nazionale dello Stato membro richiesto, qualora quest'ultimo abbia indicato tale periodo massimo allo Stato membro richiedente all'atto della trasmissione.

I dati sono bloccati, e non cancellati, quando vi sono motivi di ritenere che la loro cancellazione pregiudicherebbe gli interessi dell'interessato. I dati bloccati possono essere utilizzati o trasmessi solo per le finalità che ne hanno impedito la cancellazione.

Articolo 53

Responsabile del trattamento

1. eu-LISA è il responsabile del trattamento ai sensi dell'articolo 3, punto 12, del regolamento (UE) 2018/1725, per il trattamento dei dati personali tramite il router.
2. Europol è il responsabile del trattamento dei dati personali tramite EPRIS.

Articolo 54

Sicurezza del trattamento

1. Europol, eu-LISA e le autorità degli Stati membri garantiscono la sicurezza del trattamento dei dati personali svolto ai sensi del presente regolamento. Europol, eu-LISA e le autorità degli Stati membri cooperano nei compiti relativi alla sicurezza.
2. Fatto salvo l'articolo 33 del regolamento (UE) 2018/1725 e l'articolo 32 del regolamento (UE) 2016/794, eu-LISA ed Europol adottano le misure necessarie per garantire la sicurezza rispettivamente del router e di EPRIS, nonché delle relative infrastrutture di comunicazione.
3. In particolare eu-LISA ed Europol adottano le misure necessarie, rispettivamente in merito al router e ad EPRIS, compresi un piano di sicurezza, un piano di continuità operativa e un piano di ripristino in caso di disastro, al fine di:
 - (a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani d'emergenza per la protezione delle infrastrutture critiche;
 - (b) negare alle persone non autorizzate l'accesso alle attrezzature e alle strutture utilizzate per il trattamento di dati;
 - (c) impedire che supporti di dati possano essere letti, copiati, modificati o asportati senza autorizzazione;
 - (d) impedire che i dati siano inseriti senza autorizzazione e che i dati personali registrati siano visionati, modificati o cancellati senza autorizzazione;
 - (e) impedire che i dati siano trattati, copiati, modificati o cancellati senza autorizzazione;
 - (f) impedire che persone non autorizzate usino sistemi di trattamento automatizzato di dati servendosi di attrezzature per la comunicazione di dati;
 - (g) garantire che le persone autorizzate ad accedere al router e ad EPRIS abbiano accesso solo ai dati previsti dalla loro autorizzazione di accesso, tramite identità di utente individuali ed esclusivamente con modalità di accesso riservato;

- (h) garantire che sia possibile verificare e stabilire a quali organismi possono essere trasmessi dati personali mediante attrezzature di comunicazione di dati;
- (i) garantire che sia possibile verificare e stabilire quali dati sono stati trattati nel router e in EPRIS, quando, da chi e per quale finalità;
- (j) impedire, in particolare mediante tecniche appropriate di cifratura, che, all'atto della trasmissione di dati personali dal router e da EPRIS o verso gli stessi ovvero durante il trasporto dei supporti di dati, tali dati personali possano essere letti, copiati, modificati o cancellati senza autorizzazione;
- (k) garantire che, in caso di interruzione, i sistemi installati possano essere ripristinati;
- (l) garantire l'affidabilità, accertandosi che eventuali anomalie nel funzionamento del router e dell'EPRIS siano adeguatamente segnalate;
- (m) monitorare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure organizzative relative al monitoraggio interno per garantire l'osservanza del presente regolamento e valutare le misure di sicurezza alla luce dei nuovi sviluppi tecnologici.

Articolo 55

Incidenti di sicurezza

1. È considerato incidente di sicurezza l'evento che ha o può avere ripercussioni sulla sicurezza del router o di EPRIS 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. Gli incidenti di sicurezza sono gestiti in modo tale da garantire una risposta rapida, efficace e adeguata.
3. Gli Stati membri notificano senza indebito ritardo alle proprie autorità di controllo competenti qualsiasi incidente di sicurezza.

Fatto salvo l'articolo 34 del regolamento (UE) 2016/794, Europol notifica a CERT-UE senza indebito ritardo, e in ogni caso entro 24 ore da quando ne viene a conoscenza, minacce informatiche significative, vulnerabilità significative e incidenti significativi. Dettagli tecnici adeguati e di pronta utilizzazione, concernenti minacce, vulnerabilità e incidenti a livello informatico, che consentono misure proattive di indagine, risposta a incidenti o mitigazione sono comunicati a CERT-UE senza indebito ritardo.

Qualora si verifichi un incidente di sicurezza in relazione all'infrastruttura centrale del router, eu-LISA notifica a CERT-UE senza indebito ritardo, e in ogni caso non oltre 24 ore dopo esserne venuta a conoscenza, minacce informatiche significative, vulnerabilità significative e incidenti significativi. Dettagli tecnici adeguati e di pronta utilizzazione, concernenti minacce, vulnerabilità e incidenti a livello informatico, che consentono misure proattive di indagine, risposta a incidenti o mitigazione sono comunicati a CERT-UE senza indebito ritardo.

4. Le informazioni su un incidente di sicurezza che abbia o possa avere ripercussioni sul funzionamento del router o sulla disponibilità, integrità e riservatezza dei dati sono fornite senza indugio dagli Stati membri e dalle agenzie dell'Unione interessate agli Stati membri e ad Europol e registrate secondo il piano di gestione degli incidenti stabilito da eu-LISA.

5. Le informazioni su un incidente di sicurezza che abbia o possa avere ripercussioni sul funzionamento di EPRIS o sulla disponibilità, integrità e riservatezza dei dati sono fornite senza indugio dagli Stati membri e dalle agenzie dell'Unione interessate agli Stati membri e registrate secondo il piano di gestione degli incidenti stabilito da Europol.

Articolo 56

Verifica interna

1. Gli Stati membri e le pertinenti agenzie dell'Unione provvedono affinché ciascuna autorità abilitata a usare Prüm II adotti le misure necessarie per verificare la propria conformità al presente regolamento e cooperi, se necessario, con l'autorità di controllo.

2. I titolari del trattamento adottano le misure necessarie per verificare la conformità del trattamento di dati a norma del presente regolamento, anche attraverso la verifica frequente delle registrazioni di cui agli articoli 40 e 45, e cooperare, laddove necessario, con le autorità di controllo e con il Garante europeo della protezione dei dati.

Articolo 57

Sanzioni

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

Articolo 58

Onere della prova

1. Gli Stati membri adottano le misure necessarie per garantire che le persone che si considerano vittime di discriminazione in ragione del trattamento o dello scambio dei loro dati personali non sostengano l'onere della prova. Nei casi in cui una persona ritenga di essere stata discriminata nel contesto di un confronto automatizzato effettuato a norma del presente regolamento dinanzi un organo giurisdizionale o un'altra autorità giudiziaria competente, le autorità dello Stato membro che hanno trattato i dati dimostrano la mancanza di discriminazione.

2. Il paragrafo 1 non si applica alle procedure penali.

3. Gli Stati membri non adottano misure specifiche ai sensi del paragrafo 1 nei procedimenti in cui l'istruzione dei fatti spetta a un organo giurisdizionale o a un organo giudiziario competente.

Articolo 59

Responsabilità

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

Articolo 60

Audit del Garante europeo della protezione dei dati

1. Il Garante europeo della protezione dei dati provvede affinché almeno ogni quattro anni sia svolto un audit delle operazioni di trattamento dei dati personali effettuate da eu-LISA e da Europol ai fini del presente regolamento conformemente ai pertinenti principi internazionali di audit. Una relazione su tale audit è trasmessa al Parlamento europeo, al Consiglio, alla Commissione, agli Stati membri e all'agenzia dell'Unione interessata. Europol ed eu-LISA hanno la possibilità di formulare osservazioni prima dell'adozione della relazione.
2. eu-LISA ed Europol forniscono al Garante europeo della protezione dei dati le informazioni da questo richieste, consentono al Garante europeo della protezione dei dati di accedere a tutti i documenti e alle loro registrazioni di cui agli articoli 40 e 45 e gli consentono di accedere in qualsiasi momento a tutti i loro locali.

Articolo 61

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

1. Le autorità di controllo e il Garante europeo della protezione dei dati, ciascuno nell'ambito delle proprie competenze, cooperano attivamente nell'ambito delle rispettive responsabilità e assicurano il controllo coordinato dell'applicazione del presente regolamento, in particolare se il Garante europeo della protezione dei dati o un'autorità di controllo constata notevoli differenze tra le pratiche degli Stati membri o trasferimenti potenzialmente illeciti nell'uso dei canali di comunicazione previsti dal quadro Prüm II.
2. Nei casi di cui al paragrafo 1 del presente articolo, è assicurato il controllo coordinato a norma dell'articolo 62 del regolamento (UE) 2018/1725.
3. Entro [*due anni dopo l'entrata in funzione del router e di EPRIS*], e successivamente ogni due anni, il comitato europeo per la protezione dei dati trasmette al Parlamento europeo, al Consiglio, alla Commissione, a Europol e ad eu-LISA una relazione congiunta sulle sue attività ai sensi del presente articolo. Tale relazione comprende un capitolo su ciascuno Stato membro redatto dall'autorità di controllo dello Stato membro interessato.

Articolo 62

Comunicazione di dati personali a paesi terzi e ad organizzazioni internazionali

I dati trattati ai sensi del presente regolamento non sono trasferiti o messi a disposizione di paesi terzi o di organizzazioni internazionali in maniera automatizzata.

CAPO 7
COMPETENZE

Articolo 63

Competenze degli Stati membri

1. Ciascuno Stato membro è competente per quanto segue:

- (a) la connessione all'infrastruttura del router;
- (b) l'integrazione dei sistemi e delle infrastrutture nazionali esistenti con il router;
- (c) l'organizzazione, la gestione, il funzionamento e la manutenzione della sua infrastruttura nazionale esistente e della sua connessione al router;
- (d) la connessione all'infrastruttura di EPRIS;
- (e) l'integrazione dei sistemi e delle infrastrutture nazionali esistenti con EPRIS;
- (f) l'organizzazione, la gestione, il funzionamento e la manutenzione della sua infrastruttura nazionale esistente e della sua connessione a EPRIS;
- (g) la gestione dell'accesso e le modalità di accesso al router da parte del personale debitamente autorizzato delle autorità nazionali competenti a norma del presente regolamento, nonché la creazione e l'aggiornamento periodico di un elenco di tale personale con le relative qualifiche;
- (h) la gestione dell'accesso e le modalità di accesso a EPRIS da parte del personale debitamente autorizzato delle autorità nazionali competenti a norma del presente regolamento, nonché la creazione e l'aggiornamento periodico di un elenco di tale personale con le relative qualifiche;
- (i) la gestione dell'accesso e le modalità di accesso a Eucaris da parte del personale debitamente autorizzato delle autorità nazionali competenti a norma del presente regolamento, nonché la creazione e l'aggiornamento periodico di un elenco di tale personale con le relative qualifiche;
- (j) la conferma manuale di una corrispondenza di cui all'articolo 6, paragrafo 3, all'articolo 7, paragrafo 3, all'articolo 13, paragrafo 2, all'articolo 22, paragrafo 2, e all'articolo 26, paragrafo 2;
- (k) la garanzia della disponibilità dei dati necessari per lo scambio di dati di cui agli articoli 6, 7, 13, 18, 22 e 26;
- (l) lo scambio di informazioni di cui agli articoli 6, 7, 13, 18, 22 e 26;
- (m) la cancellazione dei dati ricevuti da uno Stato membro richiesto entro 48 ore dalla notifica da parte dello Stato membro richiesto del fatto che i dati personali trasmessi erano inesatti, non più aggiornati o sono stati trasmessi illecitamente;
- (n) la conformità ai requisiti di qualità dei dati stabiliti nel presente regolamento.

2. Ciascuno Stato membro è responsabile della connessione delle proprie autorità nazionali competenti al router, ad EPRIS e ad Eucaris.

Articolo 64

Competenze di Europol

1. Europol è responsabile della gestione dell'accesso e delle modalità di accesso del proprio personale debitamente autorizzato al router, ad EPRIS e ad Eucaris a norma del presente regolamento.
2. Europol è responsabile del trattamento delle interrogazioni di dati Europol da parte del router. Europol adegua di conseguenza i propri sistemi di informazione.
3. Europol è responsabile di qualsiasi adeguamento tecnico della propria infrastruttura necessario per stabilire la connessione al router e ad Eucaris.
4. Europol è responsabile dello sviluppo di EPRIS in cooperazione con gli Stati membri. EPRIS fornisce le funzionalità di cui agli articoli da 42 a 46.

Europol provvede alla gestione tecnica di EPRIS. La gestione tecnica di EPRIS consiste nell'insieme dei compiti e delle soluzioni tecniche necessari per garantire il funzionamento dell'infrastruttura centrale di EPRIS e la fornitura ininterrotta di servizi agli Stati membri 24 ore su 24 e 7 giorni su 7 a norma del presente regolamento. Essa comprende la manutenzione e gli adeguamenti tecnici necessari per garantire che EPRIS funzioni a un livello di qualità tecnica soddisfacente, specialmente per quanto riguarda i tempi di risposta alle interrogazioni delle banche dati nazionali, conformemente alle specifiche tecniche.

5. Europol provvede alla formazione sull'uso tecnico di EPRIS.
6. Europol è responsabile delle procedure di cui agli articoli 49 e 50.

Articolo 65

Competenze di eu-LISA in fase di progettazione e sviluppo del router

1. eu-LISA garantisce che le infrastrutture centrali del router siano gestite conformemente al presente regolamento.
2. Il router è ospitato da eu-LISA nei suoi siti tecnici e fornisce le funzionalità di cui al presente regolamento nel rispetto delle condizioni di sicurezza, disponibilità, qualità e prestazione di cui all'articolo 66, paragrafo 1.
3. eu-LISA è responsabile dello sviluppo del router e degli eventuali adeguamenti tecnici necessari per il funzionamento del router.

eu-LISA non ha accesso a nessuno dei dati personali trattati tramite il router.

eu-LISA definisce la progettazione dell'architettura fisica del router, comprese le sue infrastrutture di comunicazione e le specifiche tecniche, nonché la sua evoluzione per quanto concerne l'infrastruttura centrale e l'infrastruttura di comunicazione sicura. Tale progettazione è adottata dal consiglio di amministrazione previo parere favorevole della Commissione. eu-LISA provvede anche agli adattamenti delle componenti dell'interoperabilità resi necessari dall'istituzione del router come previsto dal presente regolamento.

eu-LISA sviluppa e implementa il router non appena possibile dopo l'adozione da parte della Commissione delle misure di cui all'articolo 37, paragrafo 6.

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

4. Durante la fase di progettazione e sviluppo, il consiglio di gestione del programma di interoperabilità di cui all'articolo 54 del regolamento (UE) 2019/817 e all'articolo 54 del regolamento (UE) 2019/818 si riunisce regolarmente. Esso garantisce l'adeguata gestione della fase di progettazione e sviluppo del router.

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

Il gruppo consultivo di cui all'articolo 77 si riunisce regolarmente fino all'entrata in funzione del router. Dopo ciascuna riunione, esso riferisce al consiglio di gestione del programma di interoperabilità. Esso fornisce la consulenza tecnica a sostegno delle attività del consiglio di gestione del programma di interoperabilità e monitora lo stato di preparazione degli Stati membri.

Articolo 66

Competenze di eu-LISA in seguito all'entrata in funzione del router

1. In seguito all'entrata in funzione del router, eu-LISA è responsabile della gestione tecnica dell'infrastruttura centrale del router, compresi la manutenzione e gli sviluppi tecnologici. In cooperazione con gli Stati membri, provvede a che siano utilizzate, previa analisi costi/benefici, le migliori tecnologie disponibili. eu-LISA è inoltre responsabile della gestione tecnica dell'infrastruttura di comunicazione necessaria.

La gestione tecnica del router consiste nell'insieme dei compiti e delle soluzioni tecniche necessari per garantire il funzionamento del router e la fornitura ininterrotta di servizi agli Stati membri e alle agenzie dell'Unione 24 ore su 24 e 7 giorni su 7 a norma del presente regolamento. Essa comprende la manutenzione e gli adeguamenti tecnici necessari per garantire che il router funzioni a un livello di qualità tecnica soddisfacente, specialmente per quanto riguarda la disponibilità e i tempi di risposta per la presentazione di domande alle banche dati nazionali e ai dati Europol, conformemente alle specifiche tecniche.

Il router è sviluppato e gestito in maniera tale da garantire un accesso rapido, efficiente e controllato, la disponibilità completa e ininterrotta del router e un tempo di risposta in linea con le esigenze operative delle autorità competenti degli Stati membri e di Europol.

2. Fatto salvo l'articolo 17 dello statuto dei funzionari dell'Unione europea di cui al regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio⁴², 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.

eu-LISA non ha accesso a nessuno dei dati personali trattati tramite il router.

3. eu-LISA svolge compiti relativi alla formazione sull'uso tecnico del router.

⁴² GUL 56 del 4.3.1968, pag. 1.

MODIFICHE DI ALTRI STRUMENTI VIGENTI

Articolo 67

Modifiche delle decisioni del Consiglio 2008/615/GAI e 2008/616/GAI

1. Nella decisione 2008/615/GAI, gli articoli da 2 a 6 e il capo 2, sezioni 2 e 3, sono sostituiti per gli Stati membri vincolati dal presente regolamento a decorrere dalla data di applicazione delle disposizioni del presente regolamento relative al router di cui all'articolo 74.

Di conseguenza gli articoli da 2 a 6 e il capo 2, sezioni 2 e 3, della decisione 2008/615/GAI sono soppressi a decorrere dalla data di applicazione delle disposizioni del presente regolamento relative al router di cui all'articolo 74.

2. Nella decisione 2008/616/GAI, i capi da 2 a 5 e gli articoli 18, 20 e 21 sono sostituiti per gli Stati membri vincolati dal presente regolamento a decorrere dalla data di applicazione delle disposizioni del presente regolamento relative al router di cui all'articolo 74.

Di conseguenza i capi da 2 a 5 e gli articoli 18, 20 e 21 della decisione 2008/616/GAI sono soppressi a decorrere dalla data di applicazione delle disposizioni del presente regolamento relative al router di cui all'articolo 74.

Articolo 68

Modifiche del regolamento (UE) 2018/1726

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

- (1) è inserito il seguente articolo 13 bis:

"Articolo 13 bis

Compiti relativi al router

Con riguardo al regolamento (UE) .../... del Parlamento europeo e del Consiglio* [*il presente regolamento*], l'Agenzia svolge i compiti relativi al router che le sono conferiti da tale regolamento.

* Regolamento (UE) [numero] del Parlamento europeo e del Consiglio, del xy, relativo [titolo adottato ufficialmente] (GU L ...).";

all'articolo 17, il paragrafo 3 è sostituito dal seguente:

"3. L'agenzia ha sede a Tallinn (Estonia).

I compiti relativi allo sviluppo e alla gestione operativa di cui all'articolo 1, paragrafi 4 e 5, agli articoli da 3 a 8, e agli articoli 9, 11 e 13 bis sono svolti nel sito tecnico di Strasburgo (Francia).

Un sito di riserva in grado di assicurare il funzionamento di un sistema IT su larga scala in caso di guasto di tale sistema è installato a Sankt Johann im Pongau (Austria)."

Modifiche del regolamento (UE) 2019/817

All'articolo 6, paragrafo 2, del regolamento (UE) 2019/817 è aggiunta la seguente lettera d):

"d) un'infrastruttura di comunicazione sicura tra l'ESP e il router istituito dal regolamento (UE) .../... del Parlamento europeo e del Consiglio* [*il presente regolamento*].

* Regolamento (UE) [numero] del Parlamento europeo e del Consiglio, del xy, relativo [titolo adottato ufficialmente] (GU L ...).";

Modifiche del regolamento (UE) 2019/818

Il regolamento (UE) 2019/818 è così modificato:

(1) all'articolo 6, paragrafo 2, è aggiunta la seguente lettera d):

"d) un'infrastruttura di comunicazione sicura tra l'ESP e il router istituito dal regolamento (UE) .../... del Parlamento europeo e del Consiglio* [*il presente regolamento*].

* Regolamento (UE) [numero] del Parlamento europeo e del Consiglio, del xy, relativo [titolo adottato ufficialmente] (GU L ...).";

(2) all'articolo 39, i paragrafi 1 e 2 sono sostituiti dai seguenti:

"1. È istituito un archivio centrale di relazioni e statistiche (CRRS) al fine di sostenere gli obiettivi del SIS, dell'Eurodac e dell'ECRIS-TCN, in conformità dei rispettivi strumenti giuridici che disciplinano tali sistemi, e fornire dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati. Il CRRS sostiene anche gli obiettivi del quadro Prüm II.

2. eu-LISA istituisce, attua e ospita nei suoi siti tecnici il CRRS contenenti, separati per logica dal sistema di informazione dell'UE, i dati e le statistiche di cui all'articolo 74 del regolamento (UE) 2018/1862 e all'articolo 32 del regolamento (UE) 2019/816. eu-LISA raccoglie anche dati e statistiche dal router di cui all'articolo 65, paragrafo 1, del regolamento (UE) .../... * [*il presente regolamento*]. L'accesso al CRRS è concesso mediante un accesso sicuro controllato e specifici profili di utente, unicamente ai fini dell'elaborazione di relazioni e statistiche, alle autorità di cui all'articolo 74 del regolamento (UE) 2018/1862, all'articolo 32 del regolamento (UE) 2019/816 e all'articolo 65, paragrafo 1, del regolamento (UE) .../... * [*il presente regolamento*]."

DISPOSIZIONI FINALI

Articolo 71

Relazioni e statistiche

1. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione, di Europol e di eu-LISA ha accesso alla consultazione dei seguenti dati relativi al router, unicamente per elaborare relazioni e statistiche:

- (a) numero di interrogazioni presentate da ciascuno Stato membro e da Europol;
- (b) numero di interrogazioni per ciascuna categoria di dati;
- (c) numero di interrogazioni di ciascuna banca dati connessa;
- (d) numero di corrispondenze rispetto alla banca dati di ciascuno Stato membro per ciascuna categoria di dati;
- (e) numero di corrispondenze rispetto ai dati Europol per ciascuna categoria di dati;
- (f) numero di corrispondenze confermate in relazione alle quali sono stati scambiati dati di base; e
- (g) numero di interrogazioni dell'archivio comune di dati di identità tramite il router.

I dati non consentono l'identificazione di persone fisiche.

2. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, di Europol e della Commissione ha accesso alla consultazione dei seguenti dati relativi ad Eucaris, unicamente per elaborare relazioni e statistiche:

- (a) numero di interrogazioni presentate da ciascuno Stato membro e da Europol;
- (b) numero di interrogazioni di ciascuna banca dati connessa; e
- (c) numero di corrispondenze rispetto alla banca dati di ciascuno Stato membro;

I dati non consentono l'identificazione di persone fisiche.

3. Il personale debitamente autorizzato delle autorità competenti degli Stati membri, della Commissione e di Europol ha accesso alla consultazione dei seguenti dati relativi ad EPRIS, unicamente per elaborare relazioni e statistiche:

- (a) numero di interrogazioni presentate da ciascuno Stato membro e da Europol;
- (b) numero di interrogazioni di ciascun indice connesso; e
- (c) numero di corrispondenze rispetto alla banca dati di ciascuno Stato membro;

I dati non consentono l'identificazione di persone fisiche.

4. eu-LISA conserva i dati di cui a questi paragrafi.

I dati consentono alle autorità di cui al paragrafo 1 di ottenere relazioni e statistiche personalizzabili per migliorare l'efficienza della cooperazione in materia di contrasto.

Articolo 72

Spese

1. Le spese sostenute per l'istituzione e il funzionamento del router e di EPRIS sono a carico del bilancio generale dell'Unione.

2. Le spese sostenute in relazione all'integrazione delle infrastrutture nazionali esistenti e alle loro connessioni al router e ad EPRIS, nonché le spese sostenute in relazione alla creazione di banche dati nazionali di immagini del volto e indici nazionali dei casellari giudiziari a fini di prevenzione, indagine e accertamento di reati sono a carico del bilancio generale dell'Unione.

Sono escluse le spese seguenti:

- (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. Ciascuno Stato membro sostiene le spese derivanti dalla gestione, dall'utilizzo e dalla manutenzione dell'applicazione software Eucaris di cui all'articolo 19, paragrafo 1.

4. Ciascuno Stato membro sostiene le spese derivanti dalla gestione, dall'utilizzo e dalla manutenzione delle sue connessioni al router e ad EPRIS.

Articolo 73

Comunicazioni

1. Gli Stati membri comunicano a eu-LISA i nominativi delle rispettive autorità di cui all'articolo 36 che possono usare il router o accedervi.

2. eu-LISA comunica alla Commissione il positivo completamento dei collaudi di cui all'articolo 74, paragrafo 1, lettera b).

3. Gli Stati membri notificano alla Commissione, ad Europol e ad eu-LISA i punti di contatto nazionali.

Articolo 74

Entrata in funzione

1. La Commissione fissa, mediante atto di esecuzione, la data a decorrere dalla quale gli Stati membri e le agenzie dell'Unione possono iniziare ad utilizzare il router una volta che siano soddisfatte le condizioni seguenti:

- (a) sono state adottate le misure di cui all'articolo 37, paragrafo 6;
- (b) eu-LISA ha dichiarato il positivo completamento di un collaudo generale del router che ha effettuato in cooperazione con le autorità degli Stati membri ed Europol.

In tale atto di esecuzione la Commissione stabilisce altresì la data a decorrere dalla quale gli Stati membri e le agenzie dell'Unione devono iniziare a utilizzare il router. Tale data è fissata un anno dopo la data di cui al primo comma.

La Commissione può rinviare al massimo di un anno la data a decorrere dalla quale gli Stati membri e le agenzie dell'Unione devono iniziare a utilizzare il router qualora una valutazione dell'attuazione del router abbia dimostrato la necessità di tale rinvio. Tali atti di esecuzione sono adottati secondo la procedura di cui all'articolo 76, paragrafo 2.

2. La Commissione fissa, mediante atto di esecuzione, la data a decorrere dalla quale gli Stati membri e le agenzie dell'Unione devono iniziare ad utilizzare EPRIS una volta che siano soddisfatte le condizioni seguenti:

- (a) sono state adottate le misure di cui all'articolo 44, paragrafo 7;
- (b) Europol ha dichiarato il positivo completamento di un collaudo generale di EPRIS che ha effettuato in cooperazione con le autorità degli Stati membri.

3. La Commissione fissa, mediante atto di esecuzione, la data a decorrere dalla quale Europol deve mettere a disposizione degli Stati membri i dati biometrici provenienti da paesi terzi a norma dell'articolo 49 una volta che siano soddisfatte le condizioni seguenti:

- (a) il router è in funzione;
- (b) Europol ha dichiarato il positivo completamento di un collaudo generale della connessione che ha effettuato in cooperazione con le autorità degli Stati membri ed eu-LISA.

4. La Commissione fissa, mediante atto di esecuzione, la data a decorrere dalla quale Europol deve avere accesso ai dati conservati nelle banche dati degli Stati membri a norma dell'articolo 50 una volta che siano soddisfatte le condizioni seguenti:

- (a) il router è in funzione;
- (b) Europol ha dichiarato il positivo completamento di un collaudo generale della connessione che ha effettuato in cooperazione con le autorità degli Stati membri ed eu-LISA.

Articolo 75

Disposizioni transitorie e deroghe

1. Gli Stati membri e le agenzie dell'Unione iniziano ad applicare gli articoli da 21 a 24, l'articolo 47 e l'articolo 50, paragrafo 6, a decorrere dalla data fissata conformemente all'articolo 74, paragrafo 1, primo comma, fatta eccezione per gli Stati membri che non hanno iniziato a utilizzare il router.

2. Gli Stati membri e le agenzie dell'Unione iniziano ad applicare gli articoli da 25 a 28 e l'articolo 50, paragrafo 4, a decorrere dalla data fissata conformemente all'articolo 74, paragrafo 2.

3. Gli Stati membri e le agenzie dell'Unione iniziano ad applicare l'articolo 49 a decorrere dalla data fissata conformemente all'articolo 74, paragrafo 3.

4. Gli Stati membri e le agenzie dell'Unione iniziano ad applicare l'articolo 50, paragrafi 1, 2, 3, 5 e 7, a decorrere dalla data fissata conformemente all'articolo 74, paragrafo 4.

Articolo 76

Procedura di comitato

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

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011. Qualora il comitato non esprima alcun parere, la Commissione non adotta il progetto di

atto di esecuzione e si applica l'articolo 5, paragrafo 4, terzo comma, del regolamento (UE) n. 182/2011.

Articolo 77

Gruppo consultivo

Le competenze del gruppo consultivo sull'interoperabilità di eu-LISA sono estese al router. Tale gruppo consultivo sull'interoperabilità fornisce ad eu-LISA la competenza tecnica relativa al router, in particolare nel contesto della preparazione del programma di lavoro annuale e della relazione annuale di attività.

Articolo 78

Manuale pratico

La Commissione, in stretta cooperazione con gli Stati membri, Europol ed eu-LISA, mette a disposizione un manuale pratico per l'attuazione e la gestione del presente regolamento. Il manuale pratico fornisce orientamenti tecnici e operativi, raccomandazioni e migliori prassi. La Commissione adotta il manuale pratico sotto forma di raccomandazione.

Articolo 79

Monitoraggio e valutazione

1. eu-LISA ed Europol provvedono rispettivamente affinché siano istituite procedure per monitorare lo sviluppo del router e di EPRIS rispetto agli obiettivi relativi alla pianificazione e alle spese, nonché per monitorare il funzionamento del router e di EPRIS rispetto agli obiettivi prefissati in termini di risultati tecnici, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

2. Entro [*un anno dall'entrata in vigore del presente regolamento*] e successivamente ogni anno durante la fase di sviluppo del router, eu-LISA presenta rispettivamente al Parlamento europeo e al Consiglio una relazione sulla situazione dello sviluppo del router. Tale relazione include informazioni dettagliate sulle spese sostenute e informazioni sui rischi che possono incidere sulle spese complessive che sono a carico del bilancio generale dell'Unione a norma dell'articolo 72.

Una volta che lo sviluppo del router è completato, eu-LISA presenta 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 alle spese, giustificando eventuali scostamenti.

3. Entro [*un anno dall'entrata in vigore del presente regolamento*] e successivamente ogni anno durante la fase di sviluppo di EPRIS, Europol presenta al Parlamento europeo e al Consiglio una relazione sullo stato di avanzamento dei preparativi per l'attuazione del presente regolamento e sullo stato di avanzamento dello sviluppo di EPRIS, comprese informazioni dettagliate sulle spese sostenute e informazioni sui rischi che possono incidere sulle spese complessive che sono a carico del bilancio generale dell'Unione a norma dell'articolo 72.

Una volta che lo sviluppo di EPRIS è completato, Europol presenta 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 alle spese, giustificando eventuali scostamenti.

4. Ai fini della manutenzione tecnica, eu-LISA ed Europol hanno accesso alle informazioni necessarie riguardanti i trattamenti dei dati effettuati rispettivamente nel router e in EPRIS.

5. Due anni dopo l'entrata in funzione del router, e successivamente ogni due anni, eu-LISA presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico del router, compresa la sua sicurezza.

6. Due anni dopo l'entrata in funzione di EPRIS, e successivamente ogni due anni, Europol presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico di EPRIS, compresa la sua sicurezza.

7. Tre anni dopo l'entrata in funzione del router e di EPRIS di cui all'articolo 74, e successivamente ogni quattro anni, la Commissione presenta una valutazione globale del quadro Prüm II comprendente:

- (a) una valutazione dell'applicazione del presente regolamento;
- (b) un'analisi dei risultati conseguiti in relazione agli obiettivi del presente regolamento e della sua incidenza sui diritti fondamentali;
- (c) l'incidenza, l'efficacia e l'efficienza del quadro Prüm II e delle sue prassi di lavoro alla luce dei suoi obiettivi, del suo mandato e dei suoi compiti;
- (d) una valutazione della sicurezza del quadro Prüm II.

La Commissione trasmette tale 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.

8. Gli Stati membri ed Europol comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 2 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.

9. Gli Stati membri comunicano a Europol e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 3 e 6. Tali informazioni non mettono a repentaglio i metodi di lavoro né comprendono indicazioni sulle fonti, sui membri del personale o sulle indagini delle autorità designate.

10. Gli Stati membri, eu-LISA ed Europol comunicano alla Commissione le informazioni necessarie per redigere le valutazioni di cui al paragrafo 7. Gli Stati membri comunicano altresì alla Commissione il numero di corrispondenze confermate rispetto alla banca dati di ciascuno Stato membro per ciascuna categoria di dati.

Articolo 80

Entrata in vigore e applicabilità

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 Bruxelles, il

Per il Parlamento europeo
La presidente

Per il Consiglio
Il presidente

SCHEMA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II"), che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio

1.2. Settore/settori interessati

Settore: affari interni
Attività: sicurezza

1.3. La proposta riguarda:

- una nuova azione
- una nuova azione a seguito di un progetto pilota/un'azione preparatoria⁴³
- la proroga di un'azione esistente
- la fusione di una o più azioni verso un'altra/una nuova azione

1.4. Obiettivi

1.4.1. Obiettivi generali

In risposta alle pressanti esigenze operative e agli inviti del Consiglio a prendere in considerazione la revisione delle decisioni Prüm⁴⁴, al fine di ampliarne l'ambito di applicazione e di aggiornare i requisiti tecnici e giuridici necessari, la presente iniziativa dovrebbe rafforzare lo scambio automatizzato di dati nel contesto del quadro Prüm al fine di assistere le autorità di contrasto degli Stati membri nella lotta contro la criminalità.

1.4.2. Obiettivi specifici

L'iniziativa si propone di conseguire i seguenti obiettivi:

- 1) **obiettivo specifico I:** fornire una soluzione tecnica per uno scambio automatizzato di dati efficiente tra le autorità di contrasto dell'UE per renderle consapevoli dei dati pertinenti disponibili nella banca dati nazionale di un altro Stato membro;
- 2) **obiettivo specifico II:** garantire che i dati più pertinenti (ossia le immagini del volto e gli estratti del casellario giudiziale) delle banche dati nazionali di altri Stati membri siano messi a disposizione di tutte le autorità di contrasto competenti dell'UE;
- 3) **obiettivo specifico III:** garantire che i dati pertinenti (in termini di fonti di dati) della banca dati di Europol siano messi a disposizione delle autorità di contrasto nazionali e che Europol utilizzi i propri dati secondo il loro pieno potenziale;

⁴³ A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

⁴⁴ Decisioni 2008/615/GAI e 2008/616/GAI del Consiglio.

4) **obiettivo specifico IV:** fornire alle autorità di contrasto un accesso efficiente ai dati effettivi corrispondenti a un "hit" (riscontro positivo) disponibile nella banca dati nazionale di un altro Stato membro o presso Europol.

1.4.3. Risultati e incidenza previsti

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

L'iniziativa affronterà in maniera efficace i problemi individuati e rafforzerà l'attuale quadro Prüm con capacità aggiuntive mirate e forti destinate a intensificare il suo sostegno a favore degli Stati membri nel rafforzare lo scambio di informazioni con l'obiettivo finale di prevenire e indagare reati, anche di terrorismo, nel pieno rispetto dei diritti fondamentali.

I beneficiari finali di tutte le opzioni prescelte sono i **cittadini**, che beneficeranno direttamente e indirettamente di un **contrasto migliore della criminalità nonché di tassi di criminalità inferiori**. In termini di efficienza, i beneficiari principali sono le **autorità di contrasto nazionali**. La presente iniziativa fornisce soluzioni efficienti a sfide che altrimenti dovrebbero essere affrontate a costi più elevati o che sarebbero meno efficienti.

1.4.4. Indicatori di prestazione

Precisare gli indicatori con cui monitorare progressi e risultati

Lo sviluppo del router e di EPRIS inizierà una volta soddisfatti i prerequisiti, ossia l'adozione della proposta giuridica da parte dei colegislatori e il soddisfacimento dei prerequisiti tecnici. Mentre i lavori concernenti il router inizierebbero come un progetto nuovo, quelli concernenti l'EPRIS dovrebbero basarsi sull'attuale progetto ADEP.EPRIS.

Obiettivo specifico: operatività entro la data prevista

Entro il 2023 la proposta viene trasmessa ai colegislatori per l'adozione. Basandosi sulla tempistica di altre proposte si presume che l'iter di adozione sarà completato nel corso del 2024.

Partendo da questo presupposto, l'inizio del periodo di sviluppo è stato fissato all'inizio del 2025 (= T0), che funge da punto di riferimento per conteggiare le scadenze successive, senza date assolute. Se i colegislatori adotteranno la proposta più tardi, il calendario slitterà conseguentemente.

Lo sviluppo del router e di EPRIS dovrebbe avvenire nel 2025 e nel 2026, con un inizio delle operazioni previsto nel 2027.

Gli indicatori principali riportati di seguito consentiranno di monitorare l'attuazione e il rendimento degli obiettivi specifici.

Obiettivo specifico I: fornire una soluzione tecnica per uno scambio automatizzato efficiente di dati

- Numero di casi eseguiti (= numero di domande di interrogazioni che possono essere gestite dal router) per periodo di tempo;
- numero di casi eseguiti (= numero di domande di interrogazioni che possono essere gestite da EPRIS) per periodo di tempo.

Obiettivo specifico II: garantire la disponibilità di dati più pertinenti

- Numero di domande di interrogazioni con immagini del volto;
- numero di domande di interrogazioni con il criterio del casellario giudiziale;
- numero di corrispondenze a seguito di interrogazioni con immagini del volto;

- numero di corrispondenze a seguito di interrogazioni con il criterio del casellario giudiziale.

Obiettivo specifico III: garantire che i dati pertinenti (in termini di fonti di dati) della banca dati di Europol siano messi a disposizione delle autorità di contrasto nazionali e che Europol utilizzi i propri dati secondo il loro pieno potenziale.

- Numero di domande di interrogazioni di dati biometrici di Europol provenienti da paesi terzi;

- numero di corrispondenze rispetto ai dati biometrici di Europol provenienti da paesi terzi;

- numero di domande di interrogazioni formulate da Europol;

- numero di corrispondenze risultanti da interrogazioni formulate da Europol.

Obiettivo specifico IV: fornire alle autorità di contrasto un accesso efficiente ai dati effettivi corrispondenti a un "hit" (riscontro positivo) disponibile nella banca dati nazionale di un altro Stato membro o presso Europol.

- Numero di corrispondenze a seguito di domande di interrogazioni rispetto al numero di volte in cui è stato richiesto lo scambio di dati di fondamentali.

1.5. Motivazione della proposta/iniziativa

1.5.1. *Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa*

Le varie fasi d'attuazione dell'iniziativa legislativa richiedono misure tecniche e procedurali, a livello UE e a livello nazionale, che dovrebbero avviare l'attuazione una volta entrata in vigore la normativa riveduta. Le risorse pertinenti, in particolare le risorse umane, dovrebbero essere potenziate nel tempo in linea con le misure.

I requisiti principali in seguito all'entrata in vigore della proposta sono elencati di seguito.

Creare il router Prüm

Conseguire l'obiettivo di fornire agli utenti di Prüm II una connessione unica alle banche dati di tutti gli Stati membri e ai dati Europol per inviare domande di interrogazioni con dati biometrici.

Definire un nuovo processo di follow-up a livello UE con uno scambio semiautomatizzato di dati effettivi corrispondenti a un "hit" (riscontro positivo).

Creare/ampliare EPRIS

Conseguire l'obiettivo di fornire agli utenti di Prüm II una connessione unica alle banche dati di tutti gli Stati membri contenenti gli estratti del casellario giudiziale per l'invio di domande di interrogazioni con casellari giudiziali.

Consentire agli Stati membri di scambiare nuove categorie di dati

Consentire lo scambio di immagini del volto e di estratti del casellario giudiziale tramite Prüm II.

Consentire agli Stati membri di verificare automaticamente i dati provenienti da paesi terzi disponibili presso Europol nel contesto del quadro Prüm

Consentire agli Stati membri di verificare dati biometrici provenienti da paesi terzi tramite Prüm II.

Consentire ad Europol di verificare i dati provenienti da paesi terzi rispetto alle banche dati nazionali degli Stati membri

Consentire ad Europol di utilizzare dati provenienti da paesi terzi per effettuare consultazioni nelle banche dati degli Stati membri tramite Prüm II.

Dato che occorre conseguire tutti gli obiettivi, la soluzione completa è una combinazione di quanto sopra.

- 1.5.2. *Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.*

Le forme gravi di criminalità e il terrorismo hanno carattere transnazionale, e un'azione condotta esclusivamente a livello nazionale non può contrastarli efficacemente. Questo è il motivo per cui gli Stati membri scelgono di lavorare insieme nel quadro dell'UE per affrontare le minacce poste da questi fenomeni.

Le minacce alla sicurezza in evoluzione, trainate dai diversi modi in cui i criminali sfruttano i vantaggi che la trasformazione digitale, la globalizzazione e la mobilità comportano, richiedono anche un sostegno efficace a livello UE al lavoro delle autorità di contrasto nazionali. L'azione dell'UE offre un modo efficace ed efficiente per potenziare il sostegno a favore di Stati membri nella lotta alla criminalità grave e al terrorismo al fine di far fronte a tali minacce in evoluzione.

La proposta creerà significative economie di scala spostando i compiti e i servizi che possono essere eseguiti in modo più efficiente a livello UE, dal livello nazionale ad Europol. La proposta consente così di far fronte efficacemente a delle sfide che altrimenti dovrebbero venire affrontate a costi più elevati con una serie di 27 singoli provvedimenti nazionali, o a delle sfide che, per il loro carattere transnazionale, non avrebbero alcuna soluzione a livello nazionale.

- 1.5.3. *Insegnamenti tratti da esperienze analoghe*

Dalla valutazione delle decisioni Prüm è emerso che:

- il quadro Prüm è pertinente in considerazione delle esigenze e delle sfide attuali e future legate alla sicurezza e più precisamente alle indagini penali. La cooperazione e lo scambio di informazioni tra le autorità di contrasto degli Stati membri così come la possibilità di effettuare consultazioni e raffronti di profili DNA, impronte digitali e dati di immatricolazione dei veicoli nelle banche dati di altri Stati membri ai fini della prevenzione e dell'indagine di reati sono ritenuti di fondamentale importanza per salvaguardare la sicurezza interna dell'UE e la sicurezza dei suoi cittadini;
- il concetto delle decisioni Prüm soddisfa le esigenze di coloro che si occupano di indagini penali, delle vittime di reati, degli specialisti forensi, dei depositari di banche dati e

degli operatori della giustizia per quanto concerne le categorie di dati disponibili nel contesto del quadro;

- evitando la necessità di interrogare ciascuno Stato membro a livello bilaterale, lo scambio automatizzato di dati nel contesto del quadro Prüm consente guadagni in termini di efficienza nello scambio di informazioni in materia di contrasto nella misura in cui migliora la velocità degli scambi e riduce in una certa misura l'onere amministrativo. È stato riscontrato che tali vantaggi superano gli investimenti necessari per l'attuazione del quadro Prüm. Inoltre il sistema automatizzato Prüm consente un risparmio notevole in termini di tempo di lavoro. Tuttavia sussiste ancora un onere amministrativo relativo alla verifica dei riscontri positivi e alla preparazione di relazioni, nonché alla ricezione/trasmissione di informazioni nella seconda fase;

- dall'adozione delle decisioni Prüm nel 2008 si sono inoltre concretizzati sviluppi e cambiamenti considerevoli in termini di quadro giuridico dell'UE, esigenze operative e possibilità tecniche e forensi. Diverse iniziative e diversi sistemi dell'UE e internazionali sono stati sviluppati con l'obiettivo di facilitare lo scambio di informazioni tra autorità di contrasto. Vi sono principalmente complementarità tra le decisioni Prüm e altre normative UE/internazionali pertinenti, compreso il quadro di interoperabilità. Esistono complementarità anche in relazione a taluni dei sistemi centrali di informazione dell'UE che hanno finalità diverse. Si possono individuare sinergie potenziali per quanto riguarda Europol e il quadro di interoperabilità;

- tuttavia l'attuazione delle decisioni Prüm è stata lenta. Infatti, a quasi dieci anni dalla scadenza per l'attuazione del 26 agosto 2011, tutti gli Stati membri non hanno completato la procedura di valutazione e non sono stati stabiliti numerosi collegamenti bilaterali a causa della complessità tecnica e delle rilevanti risorse finanziarie e umane necessarie. Di conseguenza le interrogazioni non possono essere confrontate con i dati in taluni Stati membri se non è stata stabilita la relativa connessione bilaterale. Ciò ostacola la capacità di identificare i criminali e individuare i legami transfrontalieri tra i crimini, una circostanza questa che ostacola lo scambio di informazioni e il funzionamento del sistema Prüm;

- anche il fatto che il follow-up in merito a riscontri positivi nel contesto del quadro di Prüm avvenga ai sensi del diritto nazionale e quindi al di fuori dell'ambito di applicazione delle decisioni Prüm è stato menzionato come una questione che ostacola il funzionamento del sistema Prüm. In effetti, a causa delle differenze delle norme e procedure nazionali, lo scambio di dati di follow-up in merito a riscontri positivi è frammentato al punto che a volte occorrono settimane o addirittura mesi per ricevere le informazioni pertinenti alla base di un riscontro positivo.

1.5.4. *Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti*

Gli investimenti richiesti a livello dell'UE sono compatibili con il quadro finanziario pluriennale 2021-2027, con finanziamenti previsti alla voce Sicurezza e difesa e Migrazione e frontiere.

1.5.5. *Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione*

Gli stanziamenti necessari per finanziare lo sviluppo del quadro Prüm II non sono stati pianificati nel contesto degli stanziamenti del quadro finanziario pluriennale (QFP) di Europol ed eu-LISA, dato che si tratta di una proposta nuova i cui importi non erano noti al momento

della proposta. Si propone di aumentare gli stanziamenti di Europol ed eu-LISA negli anni 2024, 2025, 2026 e 2027 mediante riduzioni corrispondenti rispettivamente del Fondo Sicurezza interna e dello strumento per la gestione delle frontiere e i visti.

1.6. Durata e incidenza finanziaria della proposta/iniziativa

durata limitata

in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

incidenza finanziaria dal AAAA al AAAA

durata illimitata

attuazione con un periodo di avviamento dal 2024 al 2026;

e successivo funzionamento a pieno ritmo.

1.7. Modalità di gestione previste⁴⁵

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 affidando compiti di esecuzione del bilancio:

a organizzazioni internazionali e loro agenzie (specificare);

alla BEI e al Fondo europeo per gli investimenti;

agli organismi di cui agli articoli 70 e 71;

a organismi di diritto pubblico;

a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

alle persone incaricate di attuare azioni specifiche della PESC a norma del titolo V del TUE e indicate nel pertinente atto di base.

Osservazioni

Blocchi	Fase di sviluppo	Fase operativa	Modalità di gestione	Attuatore
Sviluppo e manutenzione (del router e di EPRIS)	X	X	Indiretta	eu-LISA Europol
Adeguamento delle banche dati di Europol	X	X	Indiretta	Europol

⁴⁵ 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	Attuatore
Sviluppo o miglioramento delle banche dati nazionali esistenti, integrazione dei sistemi nazionali	X	X	Concorrente (o diretta)	COM + Stati membri

Il periodo di sviluppo inizia nel 2024 e dura fino alla realizzazione di ciascuna parte dell'iniziativa, quindi dal 2024 al 2027.

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 adeguare i propri sistemi nazionali per connettersi al router e ad EPRIS, nonché stabilire le misure necessarie per garantire lo scambio di immagini del volto ed estratti del casellario giudiziale.

3. Gestione indiretta: eu-LISA ed Europol copriranno la parte di sviluppo degli assi di intervento in ambito informatico del progetto, ossia rispettivamente il router ed EPRIS. In tale contesto rientrerebbero tutte le modifiche necessarie alla loro architettura esistente per garantire le capacità descritte nella proposta.

Durante il periodo operativo eu-LISA ed Europol eseguiranno tutte le attività tecniche legate alla manutenzione del router e di EPRIS.

Europol si occuperà dello sviluppo e della manutenzione dei suoi sistemi per garantire che i suoi dati siano disponibili nel contesto del quadro Prüm.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

eu-LISA ed Europol provvedono rispettivamente affinché siano istituite le procedure volte a monitorare lo sviluppo del router e di EPRIS rispetto agli obiettivi relativi alla pianificazione e ai costi, nonché a monitorare il funzionamento del router e di EPRIS rispetto agli obiettivi prefissati in termini di risultati tecnici, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

Al più tardi entro un anno dall'adozione della proposta di regolamento, e successivamente ogni anno durante la fase di sviluppo del router, eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sulla situazione dello sviluppo del router. Tale relazione include informazioni dettagliate sui costi sostenuti e informazioni sui rischi che possono incidere sui costi complessivi che sono a carico del bilancio generale dell'Unione.

Una volta che lo sviluppo è completato, eu-LISA presenta 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.

Al più tardi entro un anno dall'adozione della proposta di regolamento, e successivamente ogni anno durante la fase di sviluppo di EPRIS, Europol presenta al Parlamento europeo e al Consiglio una relazione sullo stato di avanzamento dei preparativi per l'attuazione del presente regolamento, sullo stato di avanzamento dello sviluppo di EPRIS, comprese informazioni dettagliate sui costi sostenuti e informazioni sui rischi che possono incidere sui costi complessivi che sono a carico del bilancio generale dell'Unione.

Una volta che lo sviluppo di EPRIS è completato, Europol presenta 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.

Ai fini della manutenzione tecnica, eu-LISA ed Europol hanno accesso alle informazioni necessarie riguardanti i trattamenti dei dati effettuati rispettivamente nel router e in EPRIS.

Due anni dopo l'entrata in funzione del router, e successivamente ogni due anni, eu-LISA presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico del router, compresa la sua sicurezza.

Due anni dopo l'entrata in funzione di EPRIS, e successivamente ogni due anni, Europol presenta al Parlamento europeo, al Consiglio e alla Commissione una relazione sul funzionamento tecnico del router, compresa la sua sicurezza.

Tre anni dopo l'entrata in funzione di tutti gli elementi della proposta di regolamento e, successivamente ogni quattro anni, la Commissione presenta una valutazione globale del quadro Prüm II comprendente:

- a) una valutazione dell'applicazione del presente regolamento;
- b) un'analisi dei risultati conseguiti in relazione agli obiettivi del presente regolamento e della sua incidenza sui diritti fondamentali;

c) l'incidenza, l'efficacia e l'efficienza del quadro Prüm II e delle sue prassi di lavoro alla luce dei suoi obiettivi, del suo mandato e dei suoi compiti;

d) una valutazione della sicurezza del quadro Prüm II.

La Commissione trasmette tale 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.

Gli Stati membri ed Europol comunicano a eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui sopra. 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.

Gli Stati membri comunicano ad Europol e alla Commissione le informazioni necessarie per redigere le relazioni di cui sopra. 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.

eu-LISA ed Europol comunicano alla Commissione le informazioni necessarie per redigere le tue valutazioni.

2.2. Sistema di gestione e di controllo

2.2.1. *Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per i rischi*

Sono stati individuati i seguenti rischi:

- risorse operative sottoposte a pressione in ragione dell'aumento dei flussi di dati e del panorama delle attività criminali in continua evoluzione;

- nonché alla moltiplicazione dei compiti e delle richieste tanto per eu-LISA quanto per Europol;

- mancanza di livelli adeguati di risorse finanziarie e umane per rispondere alle esigenze operative;

- ritardi nei necessari sviluppi e aggiornamenti del sistema centrale a causa di mancanza di risorse TIC;

- rischi connessi al trattamento dei dati personali da parte di Europol e alla necessità di valutare e adattare regolarmente le garanzie procedurali e tecniche al fine di assicurare la protezione dei dati personali e i diritti fondamentali;

- dipendenze tra i preparativi che devono essere effettuati da eu-LISA per quanto riguarda il router e i preparativi che devono essere effettuati dagli Stati membri e da Europol per quanto riguarda la creazione di un'interfaccia tecnica per la trasmissione dei dati tramite il router.

Tali 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, in particolare:

1. 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;
3. il rischio che il contraente sperimenti difficoltà finanziarie per ragioni esterne al progetto.

Tali rischi sono attenuati aggiudicando i contratti in base a criteri di qualità rigorosi, verificando le referenze 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.

Europol attua uno specifico quadro di controllo interno basato sul quadro di controllo interno della Commissione europea e sul quadro di controllo interno integrato del comitato delle organizzazioni sponsorizzatrici originario. Il documento unico di programmazione deve fornire informazioni sui sistemi di controllo interno, mentre la relazione annuale di attività consolidata (RAAC) deve contenere informazioni sull'efficienza e l'efficacia di tali sistemi di controllo interno, anche per quanto riguarda la valutazione dei rischi. La RAAC 2019 riferisce che, sulla base dell'analisi delle componenti e dei principi del controllo interno monitorati nel corso del 2019, utilizzando elementi tanto quantitativi quanto qualitativi, il sistema di controllo interno di Europol è valutato come presente e funzionante in modo integrato in tutta l'Agenzia.

Per il bilancio eseguito da eu-LISA è necessario un quadro di controllo interno specifico basato sul quadro di controllo interno della Commissione europea. Il documento unico di programmazione deve fornire informazioni sui sistemi di controllo interno, mentre la RAAC deve contenere informazioni sull'efficienza e l'efficacia di tali sistemi di controllo interno, anche per quanto riguarda la valutazione dei rischi. La RAAC 2019 riferisce che la dirigenza dell'Agenzia ha la ragionevole certezza che siano stati predisposti controlli interni adeguati e che stiano funzionando secondo le aspettative, e che, nel corso dell'anno, i rischi più gravi siano stati opportunamente individuati e gestiti. Tale garanzia è ulteriormente confermata dai risultati degli audit interni ed esterni effettuati nel corso dell'anno.

Tanto per Europol quanto per eu-LISA, un ulteriore livello di supervisione interna è messo a disposizione anche dalla capacità di audit interno di Europol, sulla base di un piano di audit annuale, tenendo in considerazione in particolare la valutazione dei rischi in Europol. La struttura di audit interno assiste Europol nell'adempimento dei suoi obiettivi, fornendo un approccio sistematico e disciplinato per la valutazione dell'efficacia dei processi di gestione dei rischi, di controllo e di governance, e formulando raccomandazioni per il loro miglioramento.

Inoltre il Garante europeo della protezione dei dati (GEPD) e il responsabile della protezione dei dati in entrambe le agenzie (una funzione indipendente collegata direttamente al segretariato del consiglio di amministrazione) vigilano sul trattamento di dati personali da parte delle agenzie.

Infine, in quanto direzione generale partner di Europol ed eu-LISA, la DG HOME effettua ogni anno un esercizio di gestione dei rischi per individuare e valutare i potenziali rischi elevati connessi alle attività delle agenzie. I rischi considerati critici vengono riferiti ogni anno nel piano di gestione della DG HOME e sono accompagnati da un piano d'azione che definisce le azioni di mitigazione.

2.2.2. *Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)*

Sul rapporto "costi del controllo/valore dei fondi gestiti" riferisce la Commissione. La relazione annuale di attività (RAA) 2020 della DG HOME indica lo 0,21% per questo rapporto con riferimento alle entità incaricate della gestione indiretta e alle agenzie decentrate, comprese Europol ed eu-LISA.

La Corte dei conti europea ha confermato la legittimità e la regolarità dei conti annuali tanto di Eu quanto di eu-LISA per il 2019, il che implica un tasso di errore inferiore al 2 %. Non vi sono indicazioni che il tasso di errore peggiorerà nei prossimi anni.

L'articolo 80 del rispettivo regolamento finanziario di Europol e di eu-LISA prevede inoltre la possibilità, per l'Agenzia, di condividere una struttura di audit interno con altri organismi dell'Unione che operano nello stesso settore se la struttura di audit interno di un solo organismo dell'Unione non è efficiente in termini di costi.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

Le misure previste per combattere le frodi sono previste all'articolo 35 del regolamento (UE) n. 1077/2011.

Le misure di lotta contro la frode, la corruzione e altre attività illecite sono indicate, fra l'altro, all'articolo 66 del regolamento di Europol e al titolo X del regolamento finanziario di Europol.

Europol parteciperà in particolare alle attività di prevenzione delle frodi dell'Ufficio europeo per la lotta antifrode e informerà senza indugio la Commissione dei casi di presunta frode e di altre irregolarità finanziarie - in linea con la sua strategia antifrode interna.

Nel 2020 il consiglio di amministrazione ha adottato un aggiornamento della strategia antifrode di Europol.

Le misure di lotta contro la frode, la corruzione e altre attività illecite sono indicate, fra l'altro, all'articolo 50 del regolamento eu-LISA e al titolo X del regolamento finanziario di eu-LISA.

eu-LISA parteciperà in particolare alle attività di prevenzione delle frodi dell'Ufficio europeo per la lotta antifrode e informerà senza indugio la Commissione dei casi di presunta frode e di altre irregolarità finanziarie - in linea con la sua strategia antifrode interna.

Inoltre, in quanto direzione generale partner, la DG HOME ha sviluppato e attuato la propria strategia antifrode sulla base della metodologia fornita dall'OLAF. Le agenzie decentrate, comprese Europol ed eu-LISA, rientrano nel campo di applicazione di tale strategia. La RAA 2020 della DG HOME ha concluso che i processi di prevenzione e individuazione delle frodi hanno funzionato in modo soddisfacente e hanno pertanto contribuito a garantire il conseguimento degli obiettivi di controllo interno.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

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	Tipo di spesa	Partecipazione			
	Numero	Diss./Non diss. ⁴⁶	di paesi EFTA ⁴⁷	di paesi candidati ⁴⁸	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero	Diss./Non diss.	di paesi EFTA	di paesi candidati	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
5	12.02.01 – Fondo Sicurezza Interna	Diss.	NO	NO	NO	NO
5	12.01.01 - Spese di supporto per il Fondo Sicurezza interna	Non diss.	NO	NO	NO	NO
5	12.10.01 - Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol)	Non diss.	NO	NO	NO	NO
4	11.10.02 – Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA)	Non diss.	NO	NO	NO	NO

⁴⁶ Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

⁴⁷ EFTA: Associazione europea di libero scambio.

⁴⁸ Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	5	Sicurezza e difesa
---	----------	---------------------------

Europol			Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	TOTALE
Titolo 1 - Spese per il personale	Impegni	(1)		0,551	1,102	0,847	0,847	3,347
	Pagamenti	(2)		0,551	1,102	0,847	0,847	3,347
Titolo 2 - Spesa per infrastrutture e funzionamento	Impegni	(1a)		1,49	1,052	0,516	0,516	3,574
	Pagamenti	(2a)		1,49	1,052	0,516	0,516	3,574
Titolo 3 - Spese di esercizio	Impegni	(3a)						
	Pagamenti	(3b)						
TOTALE stanziamenti per Europol	Impegni	=1+1a +3a		2,041	2,154	1,363	1,363	6,921
	Pagamenti	=2+2a +3b		2,041	2,154	1,363	1,363	6,921

Osservazioni: gli stanziamenti aggiuntivi richiesti nel contesto della presente proposta per Europol saranno coperti dal Fondo Sicurezza interna alla rubrica 5.

Rubrica del quadro finanziario pluriennale	4	– Migrazione e frontiere
---	----------	---------------------------------

eu-LISA			Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	TOTALE
Titolo 1 - Spese per il personale	Impegni	(1)		0,456	0,988	1,52	1,45	4,414
	Pagamenti	(2)		0,456	0,988	1,52	1,45	4,414
Titolo 2 - Spesa per infrastrutture e funzionamento	Impegni	(1a)		4,15	3,55	1,4	0	9,1
	Pagamenti	(2a)		4,15	3,55	1,4	0	9,1
Titolo 3 - Spese di esercizio	Impegni	(3a)		0	0	1	1,2	2,2
	Pagamenti	(3b)		0	0	1	1,2	2,2
TOTALE stanziamenti per eu-LISA	Impegni	=1+1a +3a		4,606	4,538	3,92	2,65	15,714
	Pagamenti	=2+2a +3b		4,606	4,538	3,92	2,65	15,714

Osservazioni: gli stanziamenti aggiuntivi richiesti nel contesto della presente proposta per eu-LISA saranno coperti dallo strumento per la gestione delle frontiere e i visti alla rubrica 4.

Rubrica del quadro finanziario pluriennale	5	Resilienza, sicurezza e difesa
---	---	--------------------------------

DG HOME			Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	TOTALE
Fondo Sicurezza interna	Impegni	(1)		13,64	40	40		93,64
	Pagamenti	(2)		4,68	6,55	9,39		34,65
TOTALE stanziamenti per la DG HOME	Impegni			13,64	40	40		93,64
	Pagamenti			4,68	6,55	9,39		34,65

Osservazioni: gli stanziamenti richiesti nel contesto della presente proposta saranno coperti da stanziamenti già previsti nella scheda finanziaria legislativa alla base del regolamento sul Fondo Sicurezza interna. Non sono necessarie risorse finanziarie o umane supplementari.

I costi per Stato membro comprendono:

- ammodernamento della propria infrastruttura per sostenere lo scambio di servizi web e predisposizione della connessione con il router centrale, attività queste che comportano sforzi di analisi e definizione del nuovo contesto dell'architettura;
- ammodernamento della propria infrastruttura per sostenere lo scambio di servizi web e predisposizione della connessione con il router centrale;
- configurazione di un sistema di scambio di servizi web e predisposizione della connessione con il router centrale;
- progettazione di una nuova architettura nazionale e delle specifiche per garantire l'accesso ai dati nazionali attraverso le soluzioni sviluppate (router ed EPRIS);
- creazione di un nuovo indice o messa a disposizione di un indice già esistente per lo scambio di estratti del casellario giudiziale;

- creazione di una nuova banca dati di immagini del volto o messa a disposizione per lo scambio di una banca dati di immagini del volto già esistente;
- integrazione della soluzione nazionale;
- costi generici legati alla gestione del progetto.

La tabella seguente indica i costi per ciascuna categoria:

Specificare gli obiettivi e i risultati DG Home ↓	Tipo	Anno 2023		Anno 2024		Anno 2025		Anno 2026		Anno 2027		TOTALE	
		z	Costo	N. totale	Costo totale								
Router	Connessione al router delle banche dati esistenti			26	2,314	26	6,787	26	6,787			26	15,89
Immagini del volto	Creazione della nuova banca dati			13 *	2,84	13	8,329	13	8,329			13	19,5
	Connessione della banca dati al router			26	2,72	26	7,996	26	7,996			26	18,72

Estratti del casellario giudiziale	Creazione della banca dati degli estratti del casellario giudiziale e collegamento a EPRIS		26	5,763	26	16,959	26	16,959			26	39,7
Totale				13,64		40		40				93,64

*Stima degli SM che non dispongono di banca dati di immagini del volto

Rubrica del quadro finanziario pluriennale	7	"Spese amministrative"
---	----------	-------------------------------

Mio EUR (al terzo decimale)

		Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	TOTALE
DG: HOME							
• Risorse umane			0,608	0,684	0,608	0,608	2,508
• Altre spese amministrative			0,225	0,225	0,186	0,186	0,822
TOTALE DG HOME	Stanziamanti						

TOTALE stanziamenti per la RUBRICA 7 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)		0,833	0,833	0,794	0,794	3,330
--	-------------------------------------	--	-------	-------	-------	-------	--------------

Mio EUR (al terzo decimale)

		Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	TOTALE
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni		20,287	46,692	45,283	4,013	116,275
	Pagamenti		11,329	13,247	14,647	18,059	57,282

3.2.2. *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		Anno		Anno		Anno		Anno		TOTALE	
			2023		2024		2025		2026		2027			
↓	Tipo	Costo medio ⁴⁹	Numero	Costo										
Costi Europol (non legati alle risorse umane)														
- Risultato	Infrastruttura e manutenzione					0,764		0,326		0,226		0,226		1,542
- Risultato	Contraenti					0,726		0,726		0,290		0,290		2,032
COSTI TOTALI						1,490		1,052		0,516		0,516		3,574

⁴⁹ In ragione della loro specifica natura operativa, non è possibile stabilire costi unitari precisi per ciascun prodotto, né il volume esatto previsto dei prodotti, in particolare dato che taluni prodotti sono correlati ad attività di contrasto che reagiscono ad attività criminali imprevedibili.

3.2.3. 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)

Specificar e gli obiettivi e i risultati			Anno		Anno		Anno		Anno		Anno		TOTALE	
			2023		2024		2025		2026		2027			
↓	Tipo	Costo medio ⁵⁰	Numero	Costo										
Costi Eu-LISA (non legati alle risorse umane)														
- Risultato	Infrastruttura ⁵¹				1,85		2,15		0,7		0			4,7
- Risultato	Contraenti ⁵²				1,4		0,7		0,7		0			2,8
- Risultato	Meccanismo di microcorrispondenza				0,9		0,7		0		0			
- Risultato	Manutenzione				0		0		1		1,2			2,2
COSTI TOTALI					4,15		3,55		2,4		1,2			11,3

⁵⁰ In ragione della loro specifica natura operativa, non è possibile stabilire costi unitari precisi per ciascun prodotto, né il volume esatto previsto dei prodotti, in particolare dato che taluni prodotti sono correlati ad attività di contrasto che reagiscono ad attività criminali imprevedibili.

⁵¹ Include hardware, software, disposizioni di rete, sicurezza.

⁵² Include servizi professionali, costi di progettazione e collaudo.

3.2.4. Incidenza prevista sulle risorse umane di Europol

3.2.4.1. Sintesi

- La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.
- La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	TOTALE
--	---------------------	---------------------	---------------------	---------------------	---------------------	---------------

Agenti temporanei - scenario di base						
Agenti temporanei – Ulteriori rispetto allo scenario di base (cumulativo)	0	0,551	1,101	0,847	0,847	3,347
Agenti temporanei - TOTALE						
Agenti contrattuali - scenario di base						
Esperti nazionali distaccati - scenario di base (progetto di richiesta di bilancio 2021)						

TOTALE solo costi aggiuntivi	0	0,551	1,101	0,847	0,847	3,347
TOTALE – compresi i costi dello scenario di base e aggiuntivi						

Fabbisogno di personale (ETP):

	Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027
Agenti temporanei – scenario di base	0	9,5	9,5	21,5	19,5
Agenti temporanei – Ulteriori rispetto allo scenario di base (cumulativo)	0	6,5	6,5	5	5
Agenti temporanei – TOTALE		16	16	26,5	24,5

Agenti contrattuali					
Esperti nazionali distaccati					
TOTALE	0	16,5	16,5	26,5	24,5

Le risorse umane necessarie per attuare gli obiettivi della presente proposta sono state stimate in collaborazione con Europol. Le stime tengono conto del previsto aumento del carico di lavoro in quanto i portatori di interessi utilizzano maggiormente i servizi di Europol nel corso del tempo, nonché del tempo necessario affinché Europol assorba le risorse al fine di evitare una situazione nella quale l'Agenzia non sarebbe in grado di eseguire pienamente il proprio contributo UE e impegnare gli stanziamenti a tempo debito.

Le risorse umane necessarie per attuare gli obiettivi della presente proposta saranno coperte in parte dal personale esistente presso Europol (scenario di base) e in parte da risorse aggiuntive (personale aggiuntivo rispetto allo scenario di base).

Nella scheda finanziaria legislativa non è previsto alcun aumento degli agenti contrattuali.

Per l'attuazione di Prüm II, le risorse necessarie per Europol possono essere suddivise in 3 categorie:

- 1) costi TIC per la connessione al router biometrico presso eu-LISA, lavori necessari di sviluppo nel contesto dei sistemi informativi di Europol per esporre i dati provenienti da terzi per le consultazioni da parte degli Stati membri e integrare le consultazioni in Prüm con i dati di terzi nell'interfaccia di consultazione unica di Europol USE-UI;
- 2) costi per il personale della direzione operazioni di Europol per lo svolgimento di consultazioni con dati provenienti da terzi e per esperti in biometria per eseguire la verifica dei riscontri positivi;
- 3) hosting di un router centrale per gli estratti del casellario giudiziale. Ciò comprenderà i costi hardware una tantum (compresi diversi ambienti per la produzione e il collaudo per gli Stati membri), personale TIC per garantire lo sviluppo e la gestione delle modifiche del software ADEP.EPRIS, collaudo con gli Stati membri, helpdesk 24 ore su 24, 7 giorni su 7 per sostenere gli Stati membri in caso di problemi. Al fine di garantire il pieno sostegno agli Stati membri, richiede la disponibilità di diversi profili di personale TIC, ad esempio coordinamento generale, ingegneri per i requisiti, sviluppatori, collaudatori, amministratori di sistema. Si prevede che sarà necessario comunque un organico leggermente superiore di personale TIC nel primo anno dopo l'entrata in funzione.

In ragione dei vincoli di sicurezza e del massimale concordato per gli agenti contrattuali, la maggior parte dei compiti relativi a Prüm deve essere svolta dal personale di Europol. È prevista l'esternalizzazione ad appaltatori di talune attività meno sensibili (collaudi, alcune attività di sviluppo).

Agenti temporanei in ETP (scenario di base + personale aggiuntivo)	2023	2024	2025	2026	2027
Gestione di progetto		1,0	1,0	0,5	0,5
Esperti (totale)		14,5	14,5	18,0	16,0
• <i>biometrica</i>		1,0	1,0	4,0	4,0
• <i>personale operativo</i>		0,5	0,5	4,0	4,0
• <i>TCI</i>		13,0	13,0	10,0	8,0
Supporto/monitoraggio dell'helpdesk		0,0	0,0	7,0	7,0
Coordinamento generale		1,0	1,0	1,0	1,0
Totale		16,5	16,5	26,5	24,5

3.2.5. Incidenza prevista sulle risorse umane di eu-LISA

3.2.5.1. Sintesi

- La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.
- La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027	TOTALE
--	--------------	--------------	--------------	--------------	--------------	--------

Agenti temporanei - scenario di base						
Agenti temporanei – Ulteriori rispetto allo scenario di base (cumulativo)		0,456	0,988	1,52	1,368	4,332
Agenti temporanei - TOTALE						
Agenti contrattuali - scenario di base						
Agenti contrattuali - aggiuntivi					0,082	0,082
Esperti nazionali distaccati - scenario di base (progetto di richiesta di bilancio 2021) ⁵³						

TOTALE solo costi aggiuntivi		0,456	0,988	1,52	1,45	4,414
TOTALE – compresi i costi dello scenario di base e aggiuntivi						

⁵³ Livelli di personale indicati nel progetto di bilancio 2021, calcolati sulla base dei costi unitari medi del personale da utilizzare per la scheda finanziaria legislativa. Una metà dello stanziamento annuale corrispondente è calcolata per l'anno di assunzione del personale.

Fabbisogno di personale (ETP):

	Anno 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027
Agenti temporanei – scenario di base					
Agenti temporanei – Ulteriori rispetto allo scenario di base (cumulativo)		6	7	10	9
Agenti temporanei – TOTALE					
Agenti contrattuali – scenario di base					
Agenti contrattuali – aggiuntivi					2
Esperti nazionali distaccati					
TOTALE		6	7	10	11

Le risorse umane necessarie per attuare gli obiettivi del nuovo mandato sono state stimate in collaborazione con eu-LISA. Le stime tengono conto del previsto aumento del carico di lavoro in quanto i portatori di interessi utilizzano maggiormente i servizi di eu-LISA nel corso del tempo, nonché del tempo necessario affinché eu-LISA assorba le risorse al fine di evitare una situazione nella quale l'Agenzia non sarebbe in grado di eseguire pienamente il proprio contributo UE e impegnare gli stanziamenti a tempo debito.

Queste stime sono basate sui seguenti livelli di organico:

	Fase								
	Analisi e progettazione			Costruzione e sviluppo			Operazioni		
Tipo di contratto	AT	AC	Totale	AT	AC	Totale	AT	AC	Totale
Profilo	N.	N.		N.	N.		N.	N.	
Architetto informatico	1		1	1		1	1		1
Gestione di collaudi	1		1	1		1	0,5		0,5
Gestione di rilasci e modifiche			0	1		1	1		1
Amministratore di rete	1		1	1		1	1		1
Gestione della sicurezza	2		2	2		2	2		2
Operatore dell'assistenza di 1° livello (24x7)			0			0		1	1

Amministratore dell'assistenza di 2° livello (24x7)			0				0		1	1
Gestione di programmi e progetti	1		1	1			1	0,5		0,5
Proprietario del prodotto			0	1			1	1		1
Esperto in biometria	1		1	1			1	1		1
Amministratore di sistema/Infra	1		1	1			1	1		1
Totale (AC+AT)	8		8	10			10	9	2	11

Profili	Anno -1 (Preparazione e progettazione)	Anno 1	Anno 2	Anno 3	Anno 4	Anno 5
Architetto informatico (AT)	1	1	1	1	1	1
Gestione di collaudi (AT)		1	1	0,5	0,5	0,5

Gestione di rilasci e modifiche (AT)			1	1	1	1
Amministratore di rete (AT)	1	1	1	1	1	1
Gestione della sicurezza (AT)	1	1	2	2	2	2
Operatore dell'assistenza di 1° livello (AC)				1	1	1
Amministratore dell'assistenza di 2° livello (24x7) – (AC)				1	1	1
Gestione di programmi e progetti (AT)	1	1	1	0,5	0,5	0,5
Proprietario del prodotto (AT)			1	1	1	1
Esperto in biometria (AT)	1	1	1	1	1	1
Amministratore di sistema/ Infrastruttura (AT)	1	1	1	1	1	1
TOTALE	6	7	10	11	11	11

3.2.5.2. Fabbisogno previsto di risorse umane per la DG partner

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 2023	Anno 2024	Anno 2025	Anno 2026	Anno 2027
• Posti della tabella dell'organico (funzionari e agenti temporanei)					
XX 01 01 01 (sede e uffici di rappresentanza della Commissione)		5	5	4	4
XX 01 01 02 (delegazioni)					
XX 01 05 01 (ricerca indiretta)					
10 01 05 01 (ricerca diretta)					
• Personale esterno (in equivalenti a tempo pieno: ETP)⁵⁴					
XX 01 02 01 (AC, END, INT della dotazione globale)					
XX 01 02 02 (AC, AL, END, INT e JPD nelle delegazioni)					
XX 01 04 jy⁵⁵	- in sede ⁵⁶				
	- nelle delegazioni				
XX 01 05 02 (AC, END, INT - ricerca indiretta)					
10 01 05 02 (AC, END, INT - ricerca diretta)					
Altre linee di bilancio (specificare)					
TOTALE		5	5	4	4

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto in parte (3 ETP) 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. La DG necessiterà inoltre di personale aggiuntivo (2 ETP).

⁵⁴ AC = agente contrattuale; AL = agente locale; ESP = esperto nazionale distaccato; INT = personale interinale; JPD = giovane professionista in delegazione.

⁵⁵ Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

⁵⁶ Principalmente per i fondi strutturali, il Fondo europeo agricolo per lo sviluppo rurale (FEASR) e il Fondo europeo per la pesca (FEP).

Descrizione dei compiti da svolgere:

Cinque 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, mantenere aggiornato il diritto derivato, compreso qualsiasi sviluppo relativo alle norme. Poiché il programma costituisce un'attività aggiuntiva rispetto al carico di lavoro attuale, occorre personale supplementare (2 ETP). Uno degli aumenti di personale è limitato in termini di durata e riguarda soltanto il periodo di sviluppo; il secondo rappresenta l'assorbimento dei compiti del segretariato del Consiglio: dato che le decisioni del Consiglio si trasformano in un regolamento, la Commissione deve subentrare nei compiti affidati al segretariato del Consiglio e il relativo carico di lavoro è di 1 ETP.

3.2.6. *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.

- La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale⁵⁷.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

[...]

3.2.7. *Partecipazione di terzi al finanziamento*

La proposta/iniziativa non prevede cofinanziamenti da terzi.

La proposta/iniziativa prevede il cofinanziamento indicato di seguito:

Mio EUR (al terzo decimale)

	Anno N	Anno N+1	Anno N+2	Anno N+3	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			Totale
Specificare l'organismo di cofinanziamento								
TOTALE stanziamenti cofinanziati								

⁵⁷ Cfr. gli articoli 11 e 17 del regolamento (UE, Euratom) n. 1311/2013 del Consiglio, che stabilisce il quadro finanziario pluriennale per il periodo 2014-2020.

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
- su altre entrate
- indicare se le entrate sono destinate a linee di spesa specifiche

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanzamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa ⁵⁸				
		Anno N	Anno N+1	Anno N+2	Anno N+3	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)
Articolo						

Per quanto riguarda le entrate varie con destinazione specifica, precisare la o le linee di spesa interessate.

[...]

Precisare il metodo di calcolo dell'incidenza sulle entrate.

[...]

⁵⁸ Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.

ALLEGATO 5

**della
DECISIONE DELLA COMMISSIONE**

**relativa alle norme interne sull'esecuzione del bilancio generale dell'Unione europea
(sezione Commissione europea) a uso dei servizi della Commissione**

**ALLEGATO
della SCHEDA FINANZIARIA LEGISLATIVA**

ALLEGATO **della SCHEDA FINANZIARIA LEGISLATIVA**

Denominazione della proposta:

Proposta sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II"), che modifica i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 e abroga le decisioni del Consiglio 2008/615/GAI e 2008/616/GAI

- 1. QUANTITÀ E COSTO DELLE RISORSE UMANE CONSIDERATE NECESSARIE**
- 2. COSTO DELLE ALTRE SPESE AMMINISTRATIVE**
- 3. TOTALE COSTI AMMINISTRATIVI**
- 4. METODI DI CALCOLO UTILIZZATI PER STIMARE I COSTI**
 - 4.1. Risorse umane**
 - 4.2. Altre spese amministrative**

Il presente allegato accompagna la scheda finanziaria legislativa nel corso della consultazione interservizi.

Le tabelle di dati sono utilizzate per compilare le tabelle contenute nella scheda finanziaria legislativa. Esse sono esclusivamente destinate ad uso interno della Commissione.

(1) Costo delle risorse umane considerate necessarie

La proposta/iniziativa non comporta l'utilizzo di risorse umane

La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Mio EUR (al terzo decimale)

RUBRICA 7 del quadro finanziario pluriennale		2024		2025		2026		2027								TOTALE	
		ETP	Stanzamenti	ETP	Stanzamenti	ETP	Stanzamenti	ETP	Stanzamenti	ETP	Stanzamenti	ETP	Stanzamenti	ETP	Stanzamenti	ETP	Stanzamenti
• Posti della tabella dell'organico (funzionari e agenti temporanei)																	
20 01 02 01 - Sede e uffici di rappresentanza	AD	5	0,608	5	0,684	4	0,608	4	0,608							4	2,508
	AST																
20 01 02 03 - Delegazioni dell'Unione	AD																
	AST																
• Personale esterno⁵⁹																	
20 02 01 e 20 02 02 – Personale esterno – Sede e uffici di rappresentanza	AC																
	END																
	INT																

⁵⁹ AC = agente contrattuale; AL = agente locale; ESP = esperto nazionale distaccato; INT = personale interinale; JPD = giovane professionista in delegazione.

20 02 03 - Personale esterno - Delegazioni dell'Unione	AC																
	AL																
	END																
	INT																
	JPD																
Altre linee di bilancio legate alle risorse umane (<i>specificare</i>)																	
Totale parziale Risorse umane – RUBRICA 7		5	0,608	5	0,684	4	0,608	4	0,608							4	2,508

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.

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.

(2) Costo delle altre spese amministrative

- La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi
 La proposta/iniziativa comporta l'utilizzazione di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

RUBRICA 7 del quadro finanziario pluriennale	2024	2025	2026	2027				Totale
In sede o nel territorio dell'UE:								
20 02 06 01 - Spese per missioni e di rappresentanza	0,035	0,035	0,035	0,035				0,140
20 02 06 02 - Spese per conferenze e riunioni	0,125	0,125	0,125	0,125				0,500
20 02 06 03 – Comitati (Comitato Prüm II) ⁶⁰	0,065	0,065	0,026	0,026				0,182
20 02 06 04 - Studi e consultazioni								
20 04 – Spese informatiche (istituzionali) ⁶¹								
Altre linee di bilancio non legate alle risorse umane (specificare se necessario)								
Nelle delegazioni dell'Unione								
20 02 07 01 – Spese per missioni, conferenze e di rappresentanza								

⁶⁰ Comitato Prüm II, circa 10 riunioni l'anno nel 2024 e nel 2025 e 4 riunioni l'anno dopo di cui soltanto la metà è contabilizzata nei costi (dato che l'altra metà è in videoconferenza).

⁶¹ È necessario il parere del gruppo Investimenti della DG DIGIT – IT (cfr. orientamenti sul finanziamento delle tecnologie dell'informazione, C(2020) 6126 final del 10.9.2020, pag. 7).

20 02 07 02 – Perfezionamento professionale								
20 03 05 - Infrastruttura e logistica								
Altre linee di bilancio non legate alle risorse umane (specificare se necessario)								
Totale parziale - RUBRICA 7 del quadro finanziario pluriennale	0,225	0,225	0,186	0,186				0,822

Mio EUR (al terzo decimale)

Esclusa la RUBRICA 7 del quadro finanziario pluriennale	2024	2025	2026	2027				Totale
Spese di assistenza tecnica e amministrativa (<u>escluso</u> il personale esterno) dagli stanziamenti operativi (ex linee "BA")								
- in sede								
- nelle delegazioni dell'Unione								
Altre spese di gestione per la ricerca								
Spese informatiche per la politica per i programmi operativi ⁶²								

⁶² È necessario il parere del gruppo Investimenti della DG DIGIT – IT (cfr. orientamenti sul finanziamento delle tecnologie dell'informazione, C(2020) 6126 final del 10.9.2020, pag. 7).

Spese informatiche istituzionali per programmi operativi ⁶³								
Altre linee di bilancio non legate alle risorse umane (specificare se necessario)								
Totale parziale Altro – Esclusa la RUBRICA 7 del quadro finanziario pluriennale								
Totale Altre spese amministrative (tutte le rubriche del QFP)	0,225	0,225	0,186	0,186				0,822

⁶³ Questa voce comprende i sistemi amministrativi locali e i contributi al cofinanziamento dei sistemi informatici istituzionali (cfr. gli orientamenti sul finanziamento delle tecnologie dell'informazione, C(2020) 6126 final del 10.9.2020).

(3) Totale costi amministrativi (tutte le rubriche del QFP)

Mio EUR (al terzo decimale)

Sintesi	2024	2025	2026	2027				Totale
Rubrica 7 - Risorse umane	0,608	0,684	0,608	0,608				2,508
Rubrica 7 - Altre spese amministrative	0,225	0,225	0,186	0,186				0,822
Totale parziale Rubrica 7								
Esclusa la Rubrica 7 - Risorse umane								
Esclusa la Rubrica 7 - Altre spese amministrative								
Totale parziale – Altre Rubriche								
TOTALE RUBRICA 7 ed esclusa la RUBRICA 7	0,833	0,833	0,794	0,794				3,330

Gli stanziamenti amministrativi richiesti saranno coperti dagli stanziamenti già assegnati alla gestione dell'azione e/o riassegnati, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio esistenti.

4. METODI DI CALCOLO UTILIZZATI PER STIMARE I COSTI

4.1. Risorse umane

Questa parte stabilisce il metodo di calcolo utilizzato per stimare le risorse umane considerate necessarie (ipotesi sul carico di lavoro, anche in relazione agli impieghi specifici (profili professionali Sysper 2), le categorie di personale e i costi medi corrispondenti)

RUBRICA 7 del quadro finanziario pluriennale

NB: i costi medi per ciascuna categoria di personale in sede sono disponibili sul sito BudgWeb:

https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx

Funzionari e agenti temporanei

In linea con la circolare della DG BUDGET a RUF/2020/23 del 30/11/2020 (cfr. allegato 1, Ares(2020)7207955 del 30.11.2020), 1 AD rappresenta un costo di 152 000 EUR l'anno. Una metà dello stanziamento annuale corrispondente è calcolata per l'anno di assunzione del personale.

Il fabbisogno di risorse umane è coperto in parte (3 ETP) 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. La DG necessiterà inoltre di personale aggiuntivo (2 ETP).

Descrizione dei compiti da svolgere:

Cinque 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, mantenere aggiornato il diritto derivato, compreso qualsiasi sviluppo relativo alle norme. Poiché il programma costituisce un'attività aggiuntiva rispetto al carico di lavoro attuale, occorre personale supplementare (2 ETP). Uno degli aumenti di personale è limitato in termini di durata e riguarda soltanto il periodo di sviluppo; il secondo rappresenta l'assorbimento dei compiti del segretariato del Consiglio: dato che le decisioni del Consiglio si trasformano in un regolamento, la Commissione deve subentrare nei compiti affidati al segretariato del Consiglio e il relativo carico di lavoro è di 1 ETP.

- Personale esterno

Esclusa la RUBRICA 7 del quadro finanziario pluriennale

- Soltanto posti a carico del bilancio della ricerca

- Personale esterno

4.2. Altre spese amministrative

*Precisare il metodo di calcolo utilizzato per ciascuna linea di bilancio,
in particolare le ipotesi su cui si basa (ad esempio, il numero di riunioni all'anno, i costi medi ecc.)*

RUBRICA 7 del quadro finanziario pluriennale

Si stima che si svolgeranno in media 35 missioni l'anno, comprese le missioni per le riunioni statutarie (gruppo consultivo, gruppi di lavoro di eu-LISA ed Europol e riunioni relative a EPRIS ed Eucaris), per partecipare a riunioni e conferenze relative a Prüm. Il costo unitario per missione è calcolato in base al viaggio di 1 funzionario per una media di 2 giorni per ciascuna missione ed è fissato a 500 EUR per missione al giorno.

Il costo unitario per riunione/conferenza di esperti è fissato a 25 000 EUR per 50 partecipanti. Si stima che verranno organizzate 5 riunioni l'anno.

Il costo unitario per comitato è fissato a 13 000 EUR per 26 partecipanti, ipotizzando il rimborso di 1 partecipante per Stato membro per una missione di un giorno per partecipare ai lavori del comitato. Si stima che saranno organizzate 10 riunioni l'anno nel 2024 e nel 2025 (5 in formato in presenza e 5 in formato videoconferenza) e 4 riunioni l'anno a partire dal 2026 (2 in formato in presenza e 2 in formato videoconferenza).

Esclusa la RUBRICA 7 del quadro finanziario pluriennale