Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
**Ufficio federale di polizia fedpol**

Berna, dicembre 2021

# Ordinanza sull'interoperabilità tra i sistemi di informazione Schengen/Dublino

## Ordinanza N-IOP

## Rapporto esplicativo per l'apertura della procedura di consultazione

# Indice

## 1. Situazione iniziale

I regolamenti (UE) 2019/817[1] e (UE) 2019/818[2] concernenti l'istituzione dell'interoperabilità tra i sistemi d'informazione dell'UE nei settori frontiere, migrazione e polizia sono stati approvati dal Parlamento europeo e dal Consiglio dell'UE il 20 maggio 2019 e notificati alla Svizzera il 21 maggio 2019 quali sviluppi dell'acquis di Schengen. Con l'Accordo di associazione a Schengen (AAS; RS *0.362.31*) la Svizzera si è impegnata a recepire di principio tutti i nuovi sviluppi dell'acquis di Schengen. Il decreto federale che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento dei regolamenti (UE) 2019/817 e (UE) 2019/818 (di seguito: regolamenti UE IOP) che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione dell'UE[3] è stato approvato dall'Assemblea federale nella sessione primaverile 2021. Il termine referendario è scaduto inutilizzato l'8 luglio 2021. La trasposizione di entrambi i regolamenti UE IOP ha richiesto adeguamenti a livello di legge nelle normative seguenti: legge federale sugli stranieri e la loro integrazione (LStrI), legge federale sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA), legge sulla responsabilità (LResp) e legge federale sui sistemi d'informazione di polizia della Confederazione (LSIP).

Con il presente progetto vengono sottoposte al Consiglio federale per approvazione le disposizioni a livello di ordinanza necessarie per l'attuazione dell'interoperabilità. Si tratta di disposizioni intese ad attuare a livello di ordinanza le modifiche di legge come pure le disposizioni dei regolamenti UE IOP che necessitano di essere concretizzate. Inoltre il progetto intende trasporre gli atti giuridici terziari finora notificati alla Svizzera (atti di esecuzione) in materia di interoperabilità. Da qui discende la necessità di creare una nuova ordinanza sull'interoperabilità tra i sistemi di informazione Schengen/Dublino (Ordinanza N-IOP). Le disposizioni da sancire a livello di ordinanza concernono perlopiù la protezione dei dati, la concretizzazione dei diritti di accesso ai sistemi di informazione Schengen/Dublino nonché la conservazione, l'archiviazione e la distruzione dei dati.

---

[1] 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, versione della GU L 135 del 22.5.2019, pag. 27; modificato da ultimo dal regolamento (UE) 2021/1152, GU L 249 del 14.7.2021, pag. 15.

[2] 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, versione della GU L 135 del 22.5.2019, pag. 85; modificato da ultimo dal regolamento (UE) 2021/1150, GU L 249 del 14.7.2021, pag. 1.

[3] Decreto federale che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento dei regolamenti (UE) 2019/817 e (UE) 2019/818 che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (Sviluppi dell'acquis di Schengen), FF **2021** 674

### 1.1. Aspetti generali concernenti l'interoperabilità

Con l'interoperabilità vengono introdotte in particolare quattro componenti centrali. Viene infatti creato il portale di ricerca europeo (ESP), che consente la consultazione simultanea di tutti i pertinenti sistemi di informazione dell'UE (Sistema d'informazione Schengen [SIS], sistema per il confronto dei dati relativi alle impronte digitali delle persone che hanno presentato una domanda d'asilo nonché di determinati cittadini di Paesi terzi e apolidi [Eurodac], il sistema d'informazione visti [VIS], il sistema di ingressi/uscite [EES], il sistema europeo di informazione e autorizzazione ai viaggi [ETIAS] e il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di Paesi terzi [ECRIS-TCN; non costituisce uno sviluppo di Schengen/Dublino]) nonché delle banche dati di Europol e Interpol. L'interoperabilità prevede ugualmente la registrazione a livello centralizzato dei dati biometrici e alfanumerici d'identità nell'archivio comune di dati di identità (CIR) nonché un servizio comune di confronto biometrico (sBMS). Inoltre, grazie al rilevatore di identità multiple (MID), consente di rilevare in modo efficiente le identità multiple. Tramite l'interoperabilità non vengono rilevati nuovi dati, bensì sono aggiunte nuove funzioni ai sistemi di informazione attuali (SIS, VIS, Eurodac) e futuri (EES, ETIAS, ECRIS-TCN). Nei regolamenti UE si parla di interoperabilità dei «sistemi d'informazione dell'UE». Per quanto concerne la trasposizione nel diritto svizzero, è utilizzata invece l'espressione «sistemi d'informazione Schengen/Dublino», poiché la trasposizione riguarda soltanto tali sistemi. Secondo l'agenda attuale della Commissione europea, l'sBMS sarà operativo nel maggio 2022, il CIR entro metà 2022 e l'ESP così come il MID, rispettivamente entro la metà e la fine del 2023. L'UE prevede al momento che l'entrata in funzione dell'interoperabilità avverrà per fine 2023 / inizio 2024. La data precisa sarà stabilita dalla Commissione europea in un secondo momento. Per garantire che la Svizzera sia pronta sul piano tecnico al momento dell'entrata in funzione, è previsto che l'ordinanza N-IOP entri in vigore per la fine del 2022.

### 1.2. Modifiche necessarie a livello di ordinanza

Al fine di istituire l'interoperabilità tra i sistemi di informazioni Schengen/Dublino, è necessario che le quattro componenti centrali previste siano collegate con i sistemi di informazione e le banche dati di polizia che sono in particolare disciplinati rispettivamente dalla LStrI e dalla LSIP. Per ragioni di trasparenza, le disposizioni relative alle componenti centrali sono state sancite all'interno delle suddette leggi.

L'ordinanza N-IOP intende tra l'altro attuare le nuove quattro componenti centrali. Inoltre, in futuro occorrerà apportare adeguamenti puntuali nelle altre ordinanze che disciplinano i sistemi di informazione Schengen/Dublino interessati dall'interoperabilità. Tali modifiche non fanno tuttavia parte del presente progetto e saranno sottoposte a tempo debito al Consiglio federale.

## 2. Ordinanza sull'interoperabilità tra i sistemi di informazione Schengen/Dublino (Ordinanza N-IOP)

L'ordinanza N-IOP è suddivisa in otto sezioni: Oggetto e definizioni (sezione 1: art. 1-2), Servizio comune di confronto biometrico (sezione 2: art. 3-7), Archivio comune di dati di identità (sezione 3: art. 8-17), Portale di ricerca europeo (sezione 4: art. 18-20), Rilevatore di identità multiple (sezione 5: art. 21-28), Diritti delle persone interessate (sezione 6: art. 29-30), Sicurezza dei dati (sezione 7: art. 31) e Disposizioni finali (sezione 8: art. 32).

### Sezione 1

La sezione 1 fornisce una panoramica del contenuto dispositivo per la trasposizione dell'interoperabilità tra i sistemi di informazione Schengen/Dublino ai sensi degli articoli 110-110*i* e 120*d* LStrI, 16*a*-16*f* LSIP nonché dei regolamenti UE IOP.

### Articolo 1

L'*articolo 1* descrive l'oggetto dell'ordinanza N-IOP, ossia disciplinare i diritti di consultazione nell'ESP e nel MID (lett. a), l'aggiornamento dell'sBMS (lett. b), i diritti di consultazione del CIR (lett. c), la procedura per la verifica manuale delle identità diverse nel MID (lett. d), la responsabilità per il trattamento dei dati nel MID, nel CIR e nell'sBMS (lett. e), i diritti delle persone interessate (lett. f) nonché la protezione e la sicurezza dei dati (lett. g).

### Articolo 2

L'*articolo 2* definisce le nozioni utilizzate all'interno della presente ordinanza. Suddivide i possibili collegamenti nel MID, effettuati nel quadro di una procedura di rilevazione delle identità multiple nonché dopo una verifica da parte dell'autorità competente, in collegamenti gialli (lett. a), verdi (lett. b), rossi (lett. c) e bianchi (lett. d) e rinvia per le loro definizioni alle pertinenti disposizioni dei regolamenti UE IOP (art. 30-33) che disciplinano i dettagli dei diversi collegamenti. Per quanto concerne le definizioni di «reato di terrorismo», da un lato, e di «reato grave», dall'altro, i regolamenti UE IOP e le basi giuridiche dell'UE relative al SIS rimandano rispettivamente alla direttiva (UE) 2017/541[4] e alla decisione quadro 2002/584/GAI[5]. Queste nozioni, impiegate nell'articolo 12 dell'ordinanza N-IOP, sono spiegate dettagliatamente negli allegati 1*a* e 1*b* dell'ordinanza N-SIS (RS *362.0*). È pertanto opportuno inserire nella presente ordinanza un rinvio a tali allegati (lett. e ed f). I cataloghi di reati sono stati disciplinati a livello di legge nel quadro del progetto «Prüm

[4] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, GU L 88 del 31.3.2017, pag. 6.

[5] Decisione quadro del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (2002/584/GAI), GU L 190 del 18.7.2002, pag. 1; modificata da ultimo dalla decisione quadro 2009/299/GAI, GU L 81 del 27.3.2009, pag. 24.

Plus»[6]. In un secondo momento occorrerà pertanto adeguare in tal senso il rinvio nella presente ordinanza.

**Sezione 2**

La sezione 2 contiene le disposizioni relative all'sBMS. Quest'ultimo consente di effettuare un confronto di dati biometrici trasversalmente in più sistemi di informazione Schengen/Dublino. L'sBMS registra pertanto gli elementi relativi alle caratteristiche biometriche (i cosiddetti «template biometrici») che ottiene dai dati biometrici provenienti dall'EES, dal C-VIS e dal SIS nonché, in futuro, anche dall'Eurodac. L'sBMS non costituisce una collezione di dati o «banca dati» ai sensi dell'articolo 3 lettera g della legge federale sulla protezione dei dati (LPD, RS *235.1*), in quanto i template biometrici non consentono di risalire direttamente alle persone in questione. Diversamente da quanto avviene per il SIS e il CIR, le autorità non dispongono di alcun accesso diretto all'sBMS. Poiché quest'ultimo, a differenza del CIR, è collegato anche con il SIS, il suo contenuto è stato disciplinato non solo nella LStrI (art. 110 LStrI) ma anche nella LSIP (art. 16*a* LSIP). Nonostante l'applicabilità diretta delle pertinenti disposizioni dei regolamenti UE IOP, l'sBMS è disciplinato anche a livello di legge formale per ragioni di completezza e per permettere con più facilità di effettuarvi rinvii.

**Articolo 3**

L'*articolo 3* designa la SEM e fedpol quali autorità responsabili per il trattamento dei dati nell'sBMS. La base giuridica è costituita dall'articolo 40 paragrafo 1 dei regolamenti UE IOP che attribuisce la responsabilità per il trattamento dei dati nell'sBMS alle autorità degli Stati membri responsabili rispettivamente del trattamento nell'EES, nel VIS e nel SIS. Se si tratta di dati provenienti dall'EES e dal C-VIS, il trattamento compete alla SEM. Per i dati che provengono dall'N-SIS la responsabilità è invece affidata a fedpol.

**Articolo 4**

L'*articolo 4 capoverso 1* è dedicato ai template biometrici dell'sBMS. Nello specifico statuisce che nell'sBMS sono registrati i template ottenuti dalle impronte digitali e dalle immagini del viso. La pertinente base legale è rappresentata dall'articolo 13 paragrafo 1 dei regolamenti UE IOP che disciplina la conservazione dei template biometrici nel servizio comune di confronto biometrico. Tale norma rinvia ugualmente alle basi giuridiche UE relative al SIS (dati di cui all'art. 20 par. 2

[6] Prüm Plus comprende i seguenti accordi: Accordo di partecipazione a Prüm, approvazione del Protocollo Eurodac tra la Svizzera e l'UE e dell'Accordo con gli Stati Uniti d'America nonché la loro trasposizione.

lett. w e x, esclusi i dati relativi alle impronte palmari del regolamento [UE] 2018/1862[7] e i dati di cui all'art. 4 par. 1 lett. u e v del regolamento [UE] 2018/1860[8]), all'EES (dati di cui all'art. 16 par. 1 lett. d, all'art. 17 par. 1 lett. b e c e all'art. 18 par. 2 lett. a, b e c del regolamento [UE] 2017/2226[9]) e al VIS (dati di cui all'art. 9 punto 6 del regolamento [CE] n. 767/2008[10]). Per il momento si può rinunciare a menzionare la fotografia nel testo dell'ordinanza. Infatti, se è vero che l'articolo 13 dei regolamenti UE IOP rimanda alle disposizioni dei singoli sistemi per quanto concerne i dati dai quali l'sBMS ottiene i template biometrici e che l'articolo 20 paragrafo 2 lettera w dei regolamenti (UE) 2018/1862 (SIS Polizia) e (UE) 2018/1861 (SIS Frontiere) menzioni oltre alle immagini del volto anche le fotografie, per l'UE dovranno trascorrere diversi anni prima che le fotografie possano essere contenute nell'sBMS.

L'*articolo 4 capoverso 2* prevede che i template biometrici siano conservati separati per logica in base al sistema di informazione da cui provengono, come previsto anche dall'articolo 13 paragrafo 1 dei regolamenti UE IOP.

**Articolo 5**

L'*articolo 5 capoverso 1* statuisce che l'sBMS esegue sistematicamente un confronto automatizzato con i dati biometrici registrati nel CIR e nel SIS ogniqualvolta viene creata una nuova registrazione o aggiornata una registrazione esistente nell'EES, nel C-VIS, nell'Eurodac o nel SIS. L'sBMS genera pertanto i template biometrici sulla base dei dati biometrici contenuti nel SIS e nel CIR. Le indicazioni corrispondenti nel CIR provengono da SIS, EES, C-VIS ed Eurodac (escluso solo l'ETIAS in quanto non vi vengono registrati dati biometrici). Norme dettagliate concernenti l'sBMS sono contenute nel capitolo III dei regolamenti UE IOP. I template biometrici sono inseriti nell'sBMS solo dopo che questo ha effettuato un controllo automatizzato della qualità dei dati biometrici aggiunti in uno dei sistemi di informazione Schengen/Dublino al fine di accertare il rispetto di norme minime di qualità dei dati (art. 13 par. 3 dei regolamenti UE IOP). Il confronto è

---

[7] 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; modificato da ultimo dal regolamento (UE) 2021/1150, GU L 249 del 14.7.2021, pag. 1.

[8] Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare, GU L 312 del 7.12.2018, pag. 1; modificato da ultimo dal regolamento (UE) 2021/1152, GU L 249 del 14.7.2021, pag. 15.

[9] Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011, GU L 327 del 9.12.2017, pag. 20; modificato da ultimo dal regolamento (UE) 2021/1152, GU L 249 del 14.7.2021, pag. 15.

[10] Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS), GU L 218 del 13.8.2008, pag. 60; modificato da ultimo dal regolamento (UE) 2021/1152, GU L 249 del 14.7.2021, pag. 15.

effettuato conformemente all'allegato alla decisione di esecuzione relativa all'articolo 13 paragrafo 5 dei regolamenti UE IOP come «confronto uno a uno» o come «confronto uno a molti»[11]. Il «confronto uno a uno» svolge una procedura di verifica che consente di confrontare due set di dati biometrici. Per contro, il «confronto uno a molti» serve a confrontare il template estratto dai dati biometrici immessi con i template registrati nella banca dati dell'sBMS.

L'*articolo 5 capoverso 2* stabilisce che le consultazioni sulla base di dati biometrici sono effettuate per le finalità di cui all'articolo 14 dei regolamenti UE IOP. Al riguardo l'articolo 14 rinvia anch'esso alle basi giuridiche relative al SIS, all'EES e al VIS, ovvero ai regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 e (UE) 2019/816, senza specificarli ulteriormente.

**Articolo 6**

L'*articolo 6* precisa che la durata di conservazione dei template biometrici e dei rispettivi riferimenti nell'sBMS dipende dalla conservazione dei dati biometrici nel SIS e nel CIR. Nell'sBMS sono infatti registrati i template biometrici generati in base ai dati biometrici di SIS, EES, C-VIS ed Eurodac. Il CIR costituisce una parte integrante degli ultimi tre sistemi appena menzionati. Inoltre ogni template contiene un riferimento al sistema di informazione dell'UE in cui sono conservati i corrispondenti dati biometrici e un riferimento alle registrazioni contenute in tali sistemi. Una cancellazione dei dati biometrici nel SIS o nel CIR determina la cancellazione automatica dei dati nell'sBMS. Questa disposizione è introdotta in attuazione dell'articolo 15 dei regolamenti UE IOP.

**Articolo 7**

L'*articolo 7* disciplina la verbalizzazione. Specifica che ogni consultazione di template biometrici va indicata nell'sBMS all'interno di un verbale. La verbalizzazione deve essere effettuata dalla Confederazione. La competenza specifica incombe all'autorità che ha consultato il sistema di informazione Schengen/Dublino sottostante. L'obbligo per gli Stati Schengen/Dublino di redigere verbali deriva dall'articolo 16 paragrafo 2 dei regolamenti UE IOP. Il presente articolo stabilisce pertanto le informazioni da verbalizzare: l'autorità che ha effettuato la consultazione (lett. a), i sistemi di informazione Schengen/Dublino consultati (lett. b), la data e l'ora della consultazione (lett. c), i dati biometrici usati per avviare la consultazione (lett. d) e i risultati della consultazione (lett. e). La verbalizzazione di queste informazioni garantisce che i diritti concessi in virtù della

[11] Allegato alla decisione di esecuzione della Commissione, del 26 agosto 2021, che stabilisce i requisiti di prestazione e le modalità pratiche per il monitoraggio delle prestazioni del servizio comune di confronto biometrico in applicazione dell'articolo 13, paragrafo 5, del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, C(2021) 6159 definitiva

sezione 6 della presente ordinanza possano essere effettivamente esercitati dalle persone interessate. I dati biometrici di cui alla lettera d sono i dati usati per avviare la consultazione quali le impronte digitali. I risultati della consultazione ai sensi della lettera e contengono i template biometrici.

**Sezione 3**

La sezione 3 contiene le disposizioni relative al CIR. Nel CIR viene creato un fascicolo individuale per ciascuna persona registrata nell'EES, nel C-VIS, nell'ETIAS o nell'Eurodac contenente, ove disponibili, i dati di identità, relativi ai documenti di viaggio e biometrici provenienti da questi sistemi di informazione Schengen/Dublino. Il CIR sostituisce parte del sistema centrale dei vari sistemi di informazione Schengen/Dublino (C-VIS, Eurodac, EES ed ETIAS), nella misura in cui vi vengono registrati determinati dati alfanumerici (dati di identità e dati relativi ai documenti di viaggio) e biometrici di tali sistemi di informazione. Il CIR costituisce pertanto una parte integrante di questi sistemi. I dati del SIS non sono registrati nel CIR, in quanto l'architettura del SIS si è rivelata in tal senso come eccessivamente complessa. Il CIR intende inoltre agevolare e contribuire alla corretta identificazione delle persone registrate in uno dei sistemi di informazione dell'UE summenzionati conformemente all'articolo 20 dei regolamenti UE IOP (art. 17 par. 1 dei regolamenti UE IOP). La LStrI funge da base giuridica nazionale per il CIR. Nella LStrI, nello specifico negli articoli 110*a*-110*d*, è stabilito quali dati restano nel sistema centrale del rispettivo sistema d'informazione e quali in futuro saranno invece conservati nel CIR.

**Articolo 8**

L'*articolo 8* affida alla SEM la responsabilità per il trattamento dei dati nel CIR. Infatti, conformemente all'articolo 40 paragrafo 2 dei regolamenti UE IOP la responsabilità per il trattamento dei dati nel CIR incombe all'autorità dello Stato membro responsabile del trattamento nell'EES, nel VIS e nell'ETIAS.

**Articolo 9**

L'*articolo 9 capoverso 1* statuisce che i dati di identità, relativi ai documenti di viaggio e biometrici sono registrati nel CIR separati per logica in base al sistema di informazione di provenienza conformemente all'articolo 18 paragrafo 1 dei regolamenti UE IOP.

L'*articolo 9 capoverso 2* specifica che una modifica dei dati relativi ai documenti di viaggio e dei dati biometrici di cittadini di Stati terzi nell'EES, nell'ETIAS, nel C-VIS o nell'Eurodac determina automaticamente una modifica dei dati nel CIR. Questa precisazione deriva dall'articolo 19 dei regolamenti UE IOP che disciplina l'aggiunta, la modifica e la cancellazione di dati nel CIR. Una situazione particolare si verifica quando viene creato un collegamento bianco o rosso nel MID tra

i dati dei sistemi di informazione che compongono il CIR. In questo caso il CIR non crea un nuovo fascicolo individuale, bensì aggiunge i nuovi dati al fascicolo individuale dei dati oggetto del collegamento (art. 19 par. 2 dei regolamenti UE IOP).

L'*articolo 9 capoverso 3* fa riferimento all'allegato 1 dell'ordinanza N-IOP che allestisce un catalogo dei dati basato sull'articolo 18 dei regolamenti UE IOP e menziona i dati da registrare nel CIR. Poiché il CIR costituisce un sistema di informazione, occorre elaborare un catalogo dei dati comprensivo di una matrice di consultazione. I dati da registrare nel CIR conformemente all'articolo 18 dei regolamenti UE IOP vanno suddivisi in tre categorie: generalità, dati relativi al documento di viaggio e dati biometrici. Gli articoli 10, 11 e 12 della presente ordinanza stabiliscono in quale misura le autorità sono autorizzate a consultare tali dati. I diritti di consultazione sono ugualmente riportati nell'allegato 1.

**Articolo 10**

L'*articolo 10 capoverso 1* menziona le unità organizzative della Confederazione autorizzate a consultare i dati registrati nel CIR a fini di identificazione ai sensi dell'articolo 110*b* LStrI. L'accesso al CIR a fini di identificazione è riservato alle unità organizzative che adempiono compiti di polizia. Possono infatti consultare il CIR a tale scopo fedpol, le autorità cantonali e comunali di polizia nonché l'AFD, o meglio l'Ufficio federale delle dogane e della sicurezza dei confini (UDCS) secondo la nuova denominazione ufficiale a partire dal 1° gennaio 2022, nell'ambito dei suoi compiti di natura doganale e non doganale al fine di proteggere la popolazione e salvaguardare la sicurezza interna (art. 110*b* cpv. 3 LStrI). Tali autorità vanno specificate più dettagliatamente all'interno dell'ordinanza (per garantire la certezza del diritto, analogamente a quanto avviene per altri progetti di ordinanza si fa riferimento nel limite del possibile al compito concreto anziché alla designazione attuale dell'unità). Le seguenti unità di fedpol saranno autorizzate a consultare il CIR a fini di identificazione (lett. a): la Polizia giudiziaria federale (n. 1), il Servizio federale di sicurezza (n. 2), la Centrale operativa e d'allarme (n. 3), i servizi responsabili del trattamento dei dati segnaletici di natura biometrica (n. 4) e il servizio responsabile dello scambio internazionale di informazioni di polizia in occasione di manifestazioni sportive, in relazione alla raccolta e allo scambio di informazioni allo scopo di prevenire minacce per la pubblica sicurezza o salvaguardare la sicurezza interna o esterna (n. 5). Si tratta di unità incaricate dell'esecuzione di controlli delle persone, in particolare della loro identificazione. Presso l'UDSC l'autorizzazione a consultare il CIR a fini di identificazione deve essere una prerogativa dei collaboratori incaricati del controllo delle persone (lett. b). Questa formulazione si ispira all'articolo 4 dell'ordinanza sul sistema di ingressi/uscite (OSIU; testo non ancora in vigore). Le identificazioni devono contribuire a prevenire e combattere l'immigrazione e ad assicurare un elevato livello di sicurezza (art. 2

par. 1 lett. b e c dei regolamenti UE IOP). Gli Stati Schengen/Dublino sono chiamati in tale contesto a specificare gli obiettivi di queste identificazioni (art. 20 par. 5 dei regolamenti UE IOP). Occorre pertanto evitare qualsiasi discriminazione nei confronti di cittadini di Stati terzi e garantire che siano definite le finalità esatte dell'identificazione da eseguire, che siano designate le autorità di polizia competenti e siano stabilite procedure, condizioni e criteri di tali verifiche. Questi requisiti sono già adempiuti dall'articolo 110*b* LStrI, ragion per cui non è necessaria un'ulteriore precisazione. Tutte le unità organizzative menzionate alle lettere a e b dell'articolo 10 svolgono compiti che rientrano tra gli obiettivi di cui all'articolo 2 paragrafo 1 lettere b e c dei regolamenti UE IOP.

Poiché il *capoverso 1* verte sulle unità organizzative della Confederazione, l'accesso al CIR delle autorità cantonali e comunali di polizia va disciplinato al *capoverso 2*. Questa disposizione sancisce che dette autorità sono autorizzate a consultare i dati registrati nel CIR a fini di identificazione. Essa si basa sull'articolo 110*b* capoverso 3 lettera b LStrI che concede tale diritto alle autorità cantonali e comunali di polizia.

L'*articolo 10 capoverso 3* disciplina la procedura di consultazione del CIR a fini di identificazione. La consultazione dei dati è effettuata sulla base dei dati acquisiti sul posto durante una verifica dell'identità. È necessario che la procedura venga avviata in presenza della persona interessata. Se non possono essere usati i dati biometrici dell'interessato o se la consultazione sulla base di tali dati non dà esito, la consultazione è effettuata sulla base dei dati di identità di questa persona combinati con i dati relativi al documento di viaggio oppure con i dati di identità forniti dall'interessato. Occorre evitare ogni discriminazione di cittadini di Stati terzi. Questa disposizione si basa sull'articolo 20 paragrafi 2 e 3 dei regolamenti UE IOP. Se dalla consultazione nel CIR a fini di identificazione emerge che sono registrati dati della persona interessata, l'autorità autorizzata ai sensi dei capoversi 1 e 2 riceve quale hit di tale consultazione i dati menzionati nell'allegato 1 dell'ordinanza N-IOP che sono registrati nel CIR (cfr. art. 9 cpv. 3 dell'ordinanza N-IOP). L'unità organizzativa in questione non ha tuttavia alcuna informazione in merito al sistema di informazione sottostante al CIR da cui provengono i dati.

L'*articolo 10 capoverso 4* stabilisce che in caso di catastrofi naturali, incidenti o atti violenti, le autorità autorizzate alla consultazione di cui all'articolo 10 capoverso 1 possono effettuare, ai fini dell'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o di resti umani non identificati, consultazioni nel CIR con i dati biometrici degli interessati. Ciò che si intende per «catastrofe naturale», «incidente» o «atto violento» è lasciato alla discrezione degli Stati membri, se motivi oggettivi lo giustificano. Si pensi ad esempio a una frana o a una valanga (catastrofe naturale), a un disastro aereo o a un incidente stradale (incidente) o a un omicidio (atto violento). La pertinente base giuridica è contenuta nell'articolo 20 paragrafo 4 dei regolamenti UE IOP.

## Articolo 11

L'*articolo 11* menziona le unità organizzative federali e cantonali che possono consultare i dati e i riferimenti registrati nel CIR per individuare le identità multiple ai sensi dell'articolo 110*c* LStrI. La consultazione è effettuata a fini di verifica in caso di collegamento MID giallo e al fine di combattere la frode di identità in caso di collegamento MID rosso. Le unità organizzative hanno accesso sia ai dati registrati nel CIR sia al riferimento al sistema d'informazione contenente tali dati. Sebbene l'articolo 11 rispecchi sostanzialmente il tenore dell'articolo 110*c* capoverso 1 LStrI, per ragioni di comprensibilità e completezza è opportuno ribadire tali disposizioni, vista la necessità di disciplinare tutti i diritti di accesso al CIR all'interno dell'ordinanza N-IOP. Nella misura del possibile le unità organizzative menzionate all'interno del testo di legge vengono precisate (lett. a, b n. 1., lett. c n. 1, 2 e 3). Inoltre l'Ufficio SIRENE, in virtù della lettera a, deve poter consultare per la verifica biometrica dei dati di identità, i servizi di fedpol responsabili del trattamento dei dati segnaletici di natura biometrica. Per quanto concerne invece gli aggiornamenti delle segnalazioni nel SIS inerenti al settore della migrazione è chiamata a fornire il proprio supporto la sezione Identificazione e consultazione visti della SEM (SEM-SIV), che ha la sovranità dei dati per tali informazioni. La responsabilità finale in questi casi spetta tuttavia sempre all'Ufficio SIRENE. L'articolo 11 lettera a è stato pertanto precisato in tal senso. Le unità dell'ambito direzionale Immigrazione e integrazione della SEM, responsabili del rilascio dei visti di cui alla lettera c numero 1, comprendono anche il servizio centrale di esperti del MID, creato per offrire sostegno alla verifica manuale dei collegamenti MID e che è autorizzato a consultare i dati registrati nel CIR e i pertinenti riferimenti. Il servizio centrale di esperti del MID sarà composto di collaboratori degli uffici federali. Il servizio intende fornire sostegno sul piano tecnico e del personale alle autorità responsabili della verifica manuale in casi particolarmente complessi o laddove un'autorità non disponga delle competenze necessarie per procedere alla verifica di un collegamento MID.

## Articolo 12

L'*articolo 12* elenca le unità organizzative che possono accedere al CIR ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo o altri reati gravi ai sensi dell'articolo 110*d* LStrI. Le unità menzionate possono, in concreto, consultare il CIR per appurare se vi sono registrati dati relativi a una persona specifica. Il presupposto è che nel singolo caso esistano motivi ragionevoli per ritenere che la consultazione serve alla prevenzione, all'individuazione o all'investigazione di reati di terrorismo o altri reati gravi. Se una consultazione nel CIR rivela che i dati relativi alla persona interessata sono contenuti in uno dei sistemi di informazione Schengen/Dublino, il CIR notifica alle autorità il corrispondente riferimento. Per la definizione di reati di terrorismo o di altri reati gravi si rinvia all'articolo 2 lettere e ed f dell'ordinanza N-IOP. Le consul-

tazioni del CIR ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo o altri reati gravi possono essere effettuate da fedpol, dal SIC, dal Ministero pubblico della Confederazione, dalle autorità cantonali di polizia e di perseguimento penale e dalle autorità di polizia delle Città di Zurigo, Winterthur, Losanna, Chiasso e Lugano (art. 110*d* cpv. 2 LStrI). Si tratta di autorità che adempiono compiti nel quadro della prevenzione, individuazione e investigazione di tali reati. Il capoverso 1 disciplina l'accesso di unità organizzative della Confederazione; il capoverso 2, invece, quello delle autorità cantonali di polizia e di perseguimento penale nonché dalle autorità di polizia delle Città di Zurigo, Winterthur, Losanna, Chiasso e Lugano. Le seguenti unità di fedpol devono poter consultare il CIR ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo o altri reati gravi (lett. a): la Polizia giudiziaria federale (n. 1), i servizi responsabili del trattamento dei dati segnaletici di natura biometrica (n. 2) e la Centrale operativa e d'allarme (n. 3). Presso il SIC beneficeranno di un diritto di consultazione i seguenti servizi (lett. b): la divisione Acquisizione (n. 1), la divisione Analisi (n. 2), la coordinazione Lotta al terrorismo (n. 3), la coordinazione Servizio informazioni (n. 4), la coordinazione Lotta all'estremismo (n. 5), la coordinazione Non-Proliferazione (n. 6), l'ambito Servizio degli stranieri (n. 7), l'ambito Rilevamento dati/smistamento (n. 8) e il Centro federale di situazione (n. 9). L'elenco si ispira all'articolo 12 dell'ordinanza sul sistema di ingressi/uscite (OSIU; testo non ancora in vigore) che si trova ancora in fase di elaborazione. In aggiunta alle denominazioni contenute in tale elenco il SIC ha chiesto di aggiungere anche l'ambito Rilevamento dati/smistamento e il Centro federale di situazione, che operano nel settore della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo o altri reati gravi. Presso il Ministero pubblico della Confederazione i dati nel CIR possono essere consultati ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo o altri reati gravi dalle divisioni che conducono procedimenti (lett. c). Queste ultime sono definite nell'articolo 1 capoverso 2 del regolamento del 26 febbraio 2021 sull'organizzazione e l'amministrazione del Ministero pubblico della Confederazione (RS *173.712.22*).

L'*articolo 12 capoverso 2* autorizza le autorità cantonali di polizia e di perseguimento penale e le autorità di polizia delle Città di Zurigo, Winterthur, Losanna, Chiasso e Lugano a consultare i riferimenti registrati nel CIR per gli scopi di cui al capoverso 1. La pertinente base giuridica è costituita dall'articolo 110*d* capoverso 2 lettera d LStrI.

**Articolo 13**

L'*articolo 13 capoverso 1* disciplina la prima fase della procedura a due tappe prevista dall'articolo 22 dei regolamenti UE IOP. Se durante questa prima fase emerge un riscontro positivo (ovvero se i dati relativi a una persona sono presenti in uno dei sistemi quali EES, ETIAS, C-VIS o

Eurodac), il CIR segnala all'autorità che ha effettuato la consultazione in quale sistema d'informazione sono registrati i dati. Quest'informazione può essere utilizzata esclusivamente per presentare una richiesta di accesso completo ai sensi del capoverso 2. La pertinente base giuridica è contenuta nell'articolo 110*d* capoverso 3 LStrI.

L'*articolo 13 capoverso 2* disciplina la seconda fase della procedura (art. 22 dei regolamenti UE IOP). In caso di riscontro positivo ai sensi del capoverso 1, l'autorità che ha effettuato la consultazione deve presentare alla Centrale operativa e di allarme di fedpol (EAZ fedpol) una richiesta di accesso completo ai dati di almeno uno dei sistemi di informazione che ha prodotto un riscontro positivo. L'accesso completo resta soggetto alle condizioni e alle procedure stabilite dai rispettivi strumenti giuridici che disciplinano tale accesso. La pertinente base giuridica è costituita dall'articolo 110*d* capoverso 4 LStrI. Nella richiesta occorre precisare le condizioni applicabili all'accesso completo al rispettivo sistema di informazione conformemente alle pertinenti basi giuridiche. In questo modo s'intende scongiurare ogni tentativo di abuso, e in particolare di phishing, vale a dire che un sistema possa essere consultato in assenza di motivi validi per ritenere che una persona possa esservi registrata. I motivi validi rappresentano infatti una condizione per accedere ai dati del CIR per scopi di perseguimento penale.

L'*articolo 13 capoverso 3* descrive la procedura da seguire qualora, in via eccezionale, non venga richiesto un accesso completo ai sensi del capoverso 2. In questo caso l'autorità che ha effettuato la consultazione ai sensi del capoverso 2 dell'ordinanza N-IOP nonché dell'articolo 22 paragrafo 2 dei regolamenti UE IOP è tenuta a indicare per iscritto la sua decisione e a verbalizzarla, registrando la motivazione della mancata richiesta in modo tracciabile nel fascicolo nazionale. In questo modo s'intende ugualmente prevenire ogni tentativo di phishing/abuso. La vigilanza indipendente sul trattamento dei dati è disciplinata dall'articolo 30 della presente ordinanza, in virtù del quale i diritti concessi in virtù della sezione 6 della presente ordinanza possano essere effettivamente esercitati dalle persone interessate.

**Articolo 14**

Conformemente all'*articolo 14 capoverso 1* l'EAZ fedpol, prima di approvare una richiesta di accesso completo ai dati ai sensi dell'articolo 12 capoverso 2, è tenuta a garantire che i dati possano contribuire alla prevenzione, all'individuazione e all'investigazione di reati di terrorismo o altri reati gravi (lett. a) e che sussistano prove o motivi sufficienti per ritenere che la comunicazione dei dati contribuirà a raggiungere lo scopo perseguito (lett. b). L'elenco attua l'articolo 22 paragrafo 1 dei regolamenti UE IOP che rende la consultazione del CIR possibile se vi sono motivi fondati per ritenere che contribuisca alla prevenzione, all'accertamento o all'indagine di reati di terrorismo di altri reati gravi. Segue inoltre la logica dell'articolo 14 dell'ordinanza sul sistema di ingressi/uscite (OSIU; testo non ancora in vigore), che contiene una formulazione analoga.

L'*articolo 14 capoverso 2* si richiama all'articolo 22 paragrafo 3 dei regolamenti UE IOP che sottopone il pieno accesso ai dati contenuti nell'EES, nell'ETIAS e nel C-VIS a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi alle condizioni e procedure dei rispettivi sistemi di informazioni. In concreto si tratta delle condizioni e procedure stabilite dall'articolo [...] dell'ordinanza sul sistema di ingressi/uscite (lett. a), dall'articolo [...] dell'ordinanza sul sistema europeo di informazione e autorizzazione ai viaggi (lett. b) e dall'articolo [...] dell'ordinanza sul sistema centrale d'informazione visti e sul sistema nazionale d'informazione visti (lett. c). Poiché le rispettive ordinanze di esecuzione sono attualmente in fase di elaborazione, i rinvii precisi agli articoli saranno inseriti in un secondo momento.

**Articolo 15**

L'*articolo 15* disciplina la conservazione dei dati nel CIR. In virtù dell'articolo 23 dei regolamenti UE IOP i dati conservati nel CIR vengono cancellati in modo automatizzato conformemente alle disposizioni in materia di conservazione dei dati dei rispettivi sistemi d'informazione dell'UE dai quali provengono. I fascicoli individuali sono conservati nel CIR soltanto finché i dati corrispondenti sono conservati in almeno uno dei sistemi di informazione dell'UE. Occorre prevedere che i singoli fascicoli nel CIR che rinviano ai dati contenuti nell'EES, nell'ETIAS, nel C-VIS o nell'Eurodac vengano aggiornati non appena i dati dei rispettivi sistemi sono modificati. La creazione di un collegamento non incide sul periodo di conservazione di ciascuno dei singoli dati oggetto del collegamento.

**Articolo 16**

L'*articolo 16* disciplina la verbalizzazione delle consultazioni di dati nel CIR. Vanno verbalizzate le seguenti informazioni: l'autorità che ha effettuato la consultazione (lett. a), i sistemi di informazione Schengen/Dublino consultati (lett. b), la data e l'ora della consultazione (lett. c), i dati usati per avviare la consultazione (lett. d) e i risultati della consultazione (lett. e). La base giuridica di tale obbligo è contenuta nell'articolo 24 paragrafo 5 dei regolamenti UE IOP, mentre l'enumerazione è ispirata alla struttura dell'articolo 7 della presente ordinanza. La verbalizzazione di queste informazioni garantisce che diritti concessi in virtù della sezione 6 della presente ordinanza possano essere effettivamente esercitati dalle persone interessate. In particolare occorre assicurare che la sorveglianza sul trattamento dei dati di cui all'articolo 30 della presente ordinanza sia garantita. Non esistono atti normativi di esecuzione che riguardino espressamente la verbalizzazione nel CIR. Per risultati della consultazione ai sensi della lettera e si intendono le informazioni sui sistemi di informazione Schengen/Dublino da cui provengono i dati; tali risultati non implicano la verbalizzazione di alcun dato personale.

### Articolo 17

L'*articolo 17* disciplina il diritto di informazione delle persone interessate in merito ai dati nel CIR. La pertinente base giuridica è contenuta nell'articolo 47 dei regolamenti UE IOP, il quale statuisce che l'autorità che raccoglie i dati personali da conservare nell'sBMS, nel CIR o nel MID mette a disposizione delle persone interessate le informazioni di cui agli articoli 12 e 13 della direttiva (UE) 2016/680[12] e agli articoli 15 e 16 del regolamento (UE) 2018/1725[13] usando un linguaggio semplice e chiaro[14]. A differenza del CIR o del MID, l'sBMS non costituisce una raccolta di dati o una «banca dati» ai sensi dell'articolo 3 lettera g LPD. I template biometrici contenuti nell'sBMS non sono dati personali biometrici, né vengono memorizzati in questo sistema altri dati personali (cfr. a tale riguardo l'art. 2 dell'ordinanza sul trattamento dei dati segnalatici di natura biometrica[15]). Considerato che nell'sBMS non sono registrati dati personali (bensì solo template biometrici) e che il diritto di informazione sui dati nel MID è disciplinato dall'articolo 24 capoverso 3 della presente ordinanza, nell'articolo 17 è sufficiente un rinvio al CIR. Per agevolare il flusso di informazioni con la persona interessata è creato un portale web ai sensi dell'articolo 49 dei regolamenti UE IOP.

### Sezione 4

L'ESP intende agevolare l'accesso rapido, continuato, efficace, sistematico e controllato delle autorità competenti ai diversi sistemi di informazione Schengen/Dublino e alle banche dati di Interpol conformemente ai rispettivi diritti di accesso. Le autorità competenti potranno in futuro accedere contemporaneamente, tramite un'unica consultazione e nel limite dei loro diritti d'accesso, a tutte le informazioni per esse rilevanti. La consultazione tramite l'ESP può essere effettuata sulla base di dati di identità, dati relativi ai documenti di viaggio e dati personali biometrici.

### Articolo 18

I diritti di consultazione dell'ESP non vanno disciplinati dall'ordinanza N-IOP, bensì dalle ordinanze relative ai singoli sistemi di informazione. Riguardo ai diritti di accesso delle autorità autorizzate a consultare l'ESP, l'*articolo 17 capoverso 1* rinvia pertanto ai pertinenti articoli dell'ordinanza OSIU, dell'ordinanza ETIAS, dell'ordinanza VIS (RS *142.512*) e dell'ordinanza N-SIS

---

[12] 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, versione della GU L 119 del 4.5.2016, pag. 89.

[13] 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.

[14] Il regolamento (UE) 2016/679 ugualmente menzionato all'art. 47 dei regolamenti UE IOP non fa parte dell'acquis di Schengen e non è pertanto applicabile in Svizzera.

[15] RS **361.3**

(RS *362.0*). Secondo l'articolo 110*e* capoverso 2 LStrI e l'articolo 16*b* capoverso 2 LSIP, infatti, le autorità che hanno accesso ad almeno uno dei sistemi d'informazione possono accedere, mediante procedura di richiamo, anche all'ESP. Una consultazione dei dati tramite l'ESP presuppone quindi l'autorizzazione ad accedere ad almeno uno dei sistemi di informazione Schengen/Dublino menzionati in questi articoli o a una delle banche dati di Interpol. Poiché il regolamento Eurodac riveduto non è stato ancora recepito, non è possibile per il momento rinviare all'Eurodac. Le ordinanze OSIU ed ETIAS sono attualmente in fase di elaborazione, ragion per cui le pertinenti disposizioni saranno inserite a tempo debito.

L'*articolo 18 capoverso 2* rimanda per gli ulteriori dettagli agli articoli 7 e 8 dei regolamenti UE IOP. In questo modo viene precisato che i due regolamenti UE IOP costituiscono la base per l'accesso ai dati tramite l'ESP. Entrambi gli articoli definiscono l'uso dell'ESP nonché la procedura di consultazione dell'ESP. Un elemento chiave è rappresentato dal fatto che le autorità autorizzate alla consultazione possono accedere all'ESP e ai dati da esso forniti solo per gli obiettivi e le finalità stabiliti dagli strumenti giuridici che disciplinano i sistemi di informazione nonché dai due regolamenti UE IOP. L'ESP fornisce soltanto i dati provenienti dai sistemi di informazione dell'UE e dalle banche dati di Interpol cui l'autorità che effettua la consultazione è autorizzata ad accedere.

**Articolo 19**

L'*articolo 19 capoverso 1* stabilisce le informazioni che le autorità autorizzate a consultare l'ESP ricevono in caso di riscontro positivo, ovvero l'indicazione che sono stati trovati dati (lett. a), un riferimento al sistema di informazione Schengen/Dublino o alle componenti che contengono i dati corrispondenti, laddove non si tratti di una consultazione ai sensi dell'articolo 10 (lett. b) e i dati che sono contenuti nel sistema di informazione interessato (lett. c). La pertinente base giuridica è costituita dall'articolo 9 paragrafo 4 dei regolamenti UE IOP secondo il quale la risposta contiene i dati dei sistemi di informazione cui l'autorità ha accesso nonché l'indicazione del sistema d'informazione cui appartengono i dati. La stessa disposizione esclude tuttavia la possibilità di indicare un riferimento ai sensi dell'articolo 19 capoverso 1 lettera b se si tratta di una consultazione a fini di identificazione ai sensi dell'articolo 10. L'articolo 4 paragrafo 2 delle decisioni di

esecuzione relative all'articolo 9 capoverso 7 dei regolamenti UE IOP[16] definisce il suddetto contenuto della risposta dell'ESP.

L'*articolo 19 capoverso 2* dell'ordinanza N-IOP disciplina la procedura da seguire qualora nell'ambito della consultazione dell'ESP non vengano trovati dati. In tal caso, l'ESP informa l'autorità che ha effettuato la consultazione che la consultazione è stata eseguita correttamente ma che non è stato possibile trovare alcun dato. Anche qualora si verifichi un errore, ne viene fatto menzione nella risposta dell'ESP. La pertinente base giuridica è contenuta nell'articolo 4 paragrafo 3 delle decisioni di esecuzione menzionate in precedenza, che sancisce tale obbligo.

**Articolo 20**

L'*articolo 20 capoverso 1* stabilisce che ogni consultazione di dati tramite l'ESP deve essere verbalizzata. La verbalizzazione deve essere effettuata dalla Confederazione. La competenza specifica incombe all'autorità che ha consultato il sistema di informazione Schengen/Dublino sottostante. Vanno verbalizzate le seguenti informazioni: le indicazioni sull'utente e sul profilo dell'utente che accede all'ESP (lett. a), i sistemi di informazione Schengen/Dublino e le componenti consultate (lett. b), la data e l'ora della consultazione (lett. c) e i risultati della consultazione (lett. d). La base giuridica di tale obbligo è contenuta nell'articolo 10 dei regolamenti UE IOP. L'obbligo è inoltre precisato dall'articolo 5 paragrafo 2 delle decisioni di esecuzione relative all'articolo 9 paragrafo 7 dei regolamenti UE IOP[17], che riporta lo stesso elenco. La verbalizzazione di queste informazioni garantisce che i diritti concessi in virtù della sezione 6 della presente ordinanza possano essere effettivamente esercitati dalle persone interessate. In particolare occorre provvedere affinché la sorveglianza sul trattamento dei dati di cui all'articolo 30 della presente ordinanza sia garantita.

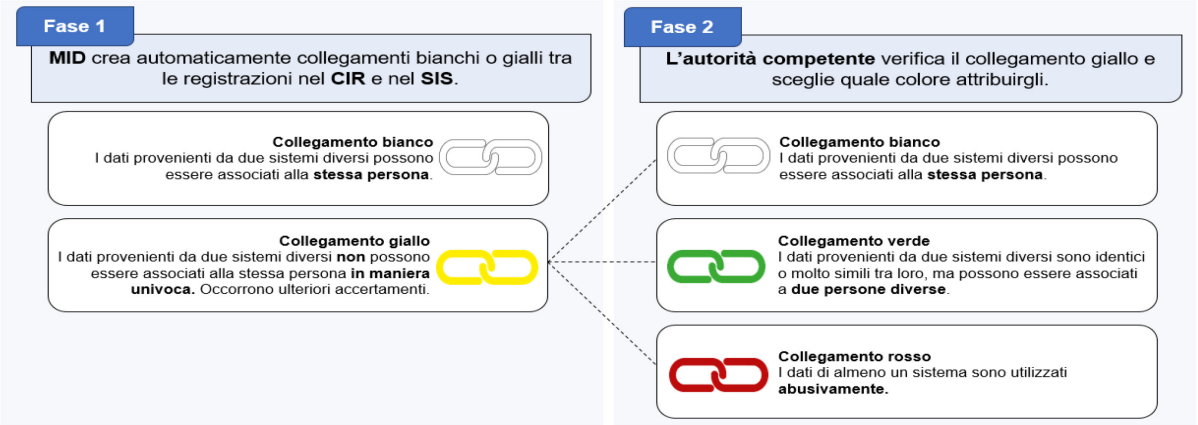
L'*articolo 20 capoverso 2* precisa che i dettagli della verbalizzazione sono retti dall'articolo 10 paragrafo 3 dei regolamenti UE IOP. Questa norma garantisce che i verbali possano essere utilizzati

[16] Decisione di esecuzione della Commissione, del 6 settembre 2021, che specifica la procedura tecnica di interrogazione da parte del portale di ricerca europeo dei sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol e il formato delle risposte del portale di ricerca europeo, a norma dell'articolo 9, paragrafo 7, del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, C(2021) 6486 definitiva; decisione di esecuzione della Commissione, del 6 settembre 2021, che specifica la procedura tecnica di interrogazione da parte del portale di ricerca europeo dei sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol e il formato delle risposte del portale di ricerca europeo, a norma dell'articolo 9, paragrafo 7, del regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, C(2021) 6484 definitiva.

[17] Decisione di esecuzione della Commissione, del 6 settembre 2021, che specifica la procedura tecnica di interrogazione da parte del portale di ricerca europeo dei sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol e il formato delle risposte del portale di ricerca europeo, a norma dell'articolo 9, paragrafo 7, del regolamento (UE) 2019/818 del Parlamento europeo e del Consigli, C(2021) 6484 definitiva; decisione di esecuzione della Commissione, del 6 settembre 2021, che specifica la procedura tecnica di interrogazione da parte del portale di ricerca europeo dei sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol e il formato delle risposte del portale di ricerca europeo, a norma dell'articolo 9, paragrafo 7, del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, C(2021) 6486 definitiva.

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. I verbali devono inoltre essere protetti dall'accesso non autorizzato con misure adeguate ed essere cancellati un anno dopo la loro creazione. Una deroga a questo termine di cancellazione è prevista laddove sia stata già avviata una procedura di monitoraggio. In tal caso, infatti, i verbali sono cancellati, se non sono più necessari per lo svolgimento di tale procedura.

**Sezione 5**




Il MID intende agevolare le verifiche di identità e contrastare le frodi di identità. Inoltre contribuisce a identificare persone che utilizzano più identità o identità fraudolente. A tale scopo, confronta i dati registrati nel CIR con quelli contenuti nel SIS. Per il confronto dei dati biometrici, il MID si serve dell'sBMS, mentre il confronto con i dati di identità e i dati relativi ai documenti di viaggio è eseguito tramite l'ESP. Nel diritto nazionale il MID è disciplinato dagli articoli 110*f* e 110*g* LStrI nonché dagli articoli 16*c* e 16*d* LSIP.

**Articolo 21**

L'*articolo 21* designa la SEM e fedpol quali autorità responsabili per il trattamento dei dati nel MID. La base giuridica è costituita dall'articolo 40 paragrafo 3 lettera b dei regolamenti UE IOP che attribuisce la responsabilità per il trattamento dei dati nel MID alle autorità degli Stati membri che aggiungono o modificano dati nel fascicolo di conferma dell'identità. Se si tratta di dati provenienti dal VIS, dall'EES e dall'ETIAS, il trattamento compete alla SEM. Per i dati che provengono dall'N-SIS la responsabilità è affidata invece a fedpol.

**Articolo 22**

L'*articolo 22 capoverso 1* rimanda, per quanto concerne lo svolgimento della procedura di rilevazione di identità multiple, all'articolo 27 dei regolamenti UE IOP che illustra tale procedura. La procedura di rilevazione è avviata quando sono registrati o aggiornati dati in uno dei sistemi di informazione Schengen/Dublino (VIS, SIS, ETIAS, EES, Eurodac). A tale scopo, sono di volta in volta confrontati i nuovi dati con i dati già presenti nel SIS e nel CIR. L'sBMS funge da strumento di confronto per i dati biometrici, mentre l'ESP serve per il confronto dei dati di identità e dei dati relativi ai documenti di viaggio.

L'*articolo 22 capoverso 2* rinvia, con riguardo agli eventuali collegamenti da creare, all'articolo 28 paragrafi 3 e 4 dei regolamenti UE IOP. Qualora dalla procedura di rilevazione risultino una o più corrispondenze, sono creati collegamenti tra i dati, nuovi o aggiornati, usati per avviare la consultazione e i dati già presenti in un altro sistema d'informazione dell'UE. Se i dati di identità, i dati relativi ai documenti di viaggio o i dati biometrici dei fascicoli oggetti del collegamento sono identici o simili, è creato automaticamente un collegamento bianco ai sensi dell'articolo 2 lettera d della presente ordinanza (lett. a). Se invece tali dati non possono essere considerati simili, è creato automaticamente un collegamento giallo ai sensi dell'articolo 2 lettera a della presente ordinanza (lett. b), che dovrà essere in seguito verificato manualmente (cfr. art. 23 della presente ordinanza).

**Articolo 23**

L'*articolo 23* descrive la procedura per la verifica manuale di un collegamento giallo. Una tale verifica va effettuata laddove esistano collegamenti tra dati di sistemi diversi e le identità non corrispondano o non si somiglino (collegamento giallo, art. 28 par. 4 dei regolamenti UE IOP). Per la procedura applicabile la Commissione adotta atti delegati, in virtù dell'articolo 28 paragrafo 5 dei regolamenti UE IOP. La verifica manuale compete all'autorità che ha registrato o aggiornato i dati nei sistemi di informazione Schengen/Dublino conformemente all'articolo 110*g* capoverso 2 LStrI. In caso di collegamenti con segnalazioni nel SIS riguardanti il settore di polizia è competente l'Ufficio SIRENE. La relativa base giuridica è costituita dall'articolo 110*f* capoverso 2 LStrI. Per sostenere la verifica manuale dei collegamenti del MID è prevista in Svizzera la creazione di un servizio centrale di esperti, che sarà composto di collaboratori degli uffici federali. Il compito del servizio sarà fornire sostegno alle autorità in casi particolarmente complessi o laddove un'autorità non disponga delle competenze necessarie per procedere alla verifica di un collegamento. La procedura di verifica manuale è retta dall'articolo 29 paragrafi 3–5 dei regolamenti UE IOP. L'autorità responsabile esegue pertanto senza indugio la verifica manuale delle identità diverse, classificando il collegamento come verde, bianco o rosso conformemente agli articoli 31–

33 dei regolamenti UE IOP. Nel campo di applicazione dell'articolo 29 paragrafo 4 del regolamento (UE) 2019/817 la verifica delle identità diverse è effettuata in presenza della persona interessata. A quest'ultima è offerta la possibilità di spiegare le circostanze all'autorità responsabile. Nel caso in cui la verifica manuale delle identità diverse sia svolta alla frontiera, essa avviene, ove possibile, entro 12 ore dalla creazione di un collegamento giallo. La creazione di un eventuale *collegamento verde* indica che i dati di identità relativi ai dati oggetto del collegamento appartengono a due persone diverse e che non sono stati utilizzati in maniera illecita. Questo può essere il caso quando i dati oggetto del collegamento evidenziano dati biometrici differenti ma gli stessi dati di identità perché due persone hanno casualmente lo stesso nome e la stessa data di nascita. Il collegamento verde permette così di facilitare il controllo dell'identità delle persone che viaggiano in modo lecito, evitando che vengano inutilmente trattenuti alla dogana per una verifica più approfondita dell'identità. Un *collegamento rosso* viene invece creato quando esistono identità multiple usate in maniera illecita oppure frodi di identità, ad esempio quando una persona utilizza più identità differenti, utilizza il documento di viaggio di un'altra persona o fa finta di essere qualcun altro. Un *collegamento bianco* viene infine creato quando i dati oggetto del collegamento si riferiscono alla stessa persona, la quale è già registrata almeno in un altro sistema di informazione dell'UE. In questo modo viene agevolata la mobilità delle persone che sono ad esempio legittimamente in possesso di più documenti di viaggio validi.

**Articolo 24**

L'*articolo 24* stabilisce le autorità che hanno accesso ai dati oggetto di un collegamento rosso, bianco o verde. Secondo il *capoverso 1*, in caso di collegamento rosso, tale diritto spetta alle autorità che hanno accesso ad almeno uno dei sistemi di informazione di cui all'articolo 110*a* LStrI o all'articolo 16*a* LSIP interessati da tale collegamento. Queste autorità sono pertanto autorizzate a consultare i dati registrati nel fascicolo di conferma dell'identità ai sensi dell'articolo 34 lettere a e b dei regolamenti UE IOP nonché dell'articolo 26 lettere a e b della presente ordinanza (v. più avanti i commenti relativi all'art. 26 che disciplina il fascicolo di conferma dell'identità). La pertinente base giuridica è costituita dall'articolo 26 paragrafo 2 dei regolamenti UE IOP.

Conformemente all'*articolo 24 paragrafo 2*, le autorità che hanno accesso ai due sistemi di informazione di cui all'articolo 110*a* LStrI o all'articolo 16*a* LSIP possono consultare, in caso di collegamento bianco, i dati registrati nel fascicolo di conferma dell'identità (v. anche commenti all'art. 26). La relativa base giuridica è rappresentata dall'articolo 26 paragrafo 3 dei regolamenti UE IOP che disciplina l'accesso ai collegamenti bianchi. La condizione è che l'autorità che effettua la consultazione abbia accesso ad entrambi i sistemi di informazione tra i quali esiste un collegamento bianco.

L'*articolo 24 paragrafo 3* disciplina l'accesso ai dati provenienti dai collegamenti in caso di un

collegamento verde. Le autorità aventi accesso ai due sistemi di informazione di cui all'articolo 110*a* LStrI o all'articolo 16*a* LSIP possono consultare i dati di cui all'articolo 26 se è emersa una corrispondenza tra i dati oggetto del collegamento. Come prevede l'articolo 26 paragrafo 4 dei regolamenti UE IOP, quale requisito, l'autorità che effettua la consultazione deve avere accesso a entrambi i sistemi di informazione tra i quali è stato creato un collegamento verde. Con riferimento ai dati concreti che possono essere consultati in caso di collegamento verde, si rinvia nuovamente all'articolo 34 dei regolamenti UE IOP nonché all'articolo 26 della presente ordinanza (in particolare il cpv. 2), contenenti precisazioni in merito al fascicolo di conferma dell'identità.

**Articolo 25**

L'*articolo 25 capoverso 1* si riallaccia alla procedura della verifica manuale di un collegamento giallo di cui all'articolo 22 della presente ordinanza e stabilisce che nel caso in cui venga creato un collegamento rosso o bianco la persona interessata debba essere informata conformemente all'articolo 32 paragrafi 4 e 5 nonché all'articolo 33 paragrafo 4 dei regolamenti UE IOP. L'autorità responsabile della verifica manuale delle identità diverse informa pertanto la persona interessata della presenza di dati di identità simili o diversi. Fornisce inoltre alla persona il numero di identificazione unico contenuto nel fascicolo di conferma dell'identità di cui all'articolo 26 della presente ordinanza, un riferimento all'autorità responsabile della verifica manuale delle identità diverse e l'indirizzo del sito web del portale istituito in virtù dell'articolo 49 dei regolamenti UE IOP. È possibile rinunciare a informare la persona interessata al fine di proteggere la sicurezza e l'ordine pubblico, di prevenire la criminalità e di garantire che non siano compromesse indagini nazionali qualora sia creato un collegamento rosso oppure in presenza di segnalazioni nel SIS secondo i regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862. Le informazioni di cui sopra vanno fornite per iscritto mediante un modulo standard. I moduli da utilizzare sono riportati all'interno delle decisioni di esecuzione che stabiliscono un modulo standard per informare le persone della creazione di un collegamento rosso o bianco[18].

L'*articolo 25 capoverso 2* disciplina la procedura da seguire quando vi sono indizi che un collegamento rosso o bianco è stato registrato in modo errato, è trattato in modo illecito o non è più aggiornato. In questi casi la procedura è retta dagli articoli 32 paragrafo 7 e 33 paragrafo 5 dei

[18] Allegato della decisione di esecuzione della Commissione che stabilisce un modulo standard per informare le persone della creazione di un collegamento rosso a norma del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, C(2021) 5988 definitiva; allegato della decisione di esecuzione della Commissione che stabilisce un modulo standard per informare le persone della creazione di un collegamento rosso a norma del regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, C(2021) 5989 definitiva; allegato della decisione di esecuzione della Commissione che stabilisce un modulo standard per informare le persone della creazione di un collegamento bianco a norma del regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, C(2021) 5620 definitiva; allegato della decisione di esecuzione della Commissione che stabilisce un modulo standard per informare le persone della creazione di un collegamento bianco a norma del regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio C(2021) 5619 definitiva

regolamenti UE IOP. La procedura differisce a seconda che si tratti di un collegamento rosso o bianco. Se un'autorità che ha accesso al CIR o al SIS ha prove che suggeriscono che un collegamento rosso è stato erroneamente registrato nel MID, controlla i dati pertinenti registrati nel CIR e nel SIS. Nel caso in cui il collegamento rosso si riferisce a una delle segnalazioni nel SIS ai sensi dell'articolo 29 paragrafo 2 dei regolamenti UE IOP, l'autorità in questione informa l'Ufficio SIRENE svizzero che, a sua volta, informa senza indugio l'Ufficio SIRENE dello Stato membro che ha creato la segnalazione nel SIS. Quest'ultimo verifica senza indugio le prove e, se del caso, rettifica o cancella il collegamento. In tutti gli altri casi l'autorità competente rettifica il collegamento errato o lo cancella dal MID. Se un'autorità con accesso al CIR dispone di prove indicanti che un collegamento bianco sia stato erroneamente registrato, deve controllare i dati pertinenti registrati nel CIR e nel SIS e, se necessario, rettificare o cancellare senza indugio il collegamento dal MID.

L'*articolo 25 capoverso 3* disciplina il diritto di informazione relativo ai dati nel MID. La base giuridica è contenuta nell'articolo 47 dei regolamenti UE IOP. Tale disposizione statuisce che l'autorità che raccoglie i dati personali da conservare nell'sBMS, nel CIR o nel MID fornisca alle persone interessate le informazioni di cui agli articoli 13 e14 della direttiva (UE) 2016/680[19] e agli articoli 15 e 16 del regolamento (UE) 2018/1725[20] usando un linguaggio semplice e chiaro[21]. Considerato che nell'sBMS non sono registrati dati personali (bensì solo template biometrici), in quanto tale servizio non costituisce una raccolta di dati o una banca dati ai sensi dell'articolo 3 lettera g LPD, e che il diritto di informazione sui dati nel CIR è disciplinato dall'articolo 17 della presente ordinanza, nell'articolo 25 capoverso 3 è sufficiente un rinvio al MID. Per agevolare il flusso di informazioni con la persona interessata è creato un portale web ai sensi dell'articolo 49 dei regolamenti UE IOP.

### Articolo 26

L'*articolo 26 capoverso 1* definisce il contenuto del fascicolo di conferma dell'identità. Se è presente un collegamento tra dati dei sistemi di informazione SIS, EES, ETIAS, C-VIS o Eurodac, nel quadro della procedura di rilevazione di identità multiple viene creato un fascicolo di conferma

---

[19] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27aprile 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; modificata da ultimo dalla rettifica della direttiva (UE) 2016/680, GU L 74 del 4.3.2021, pag. 36.

[20] 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 (Testo rilevante ai fini del SEE), GU L 295 del 21.11.2018, pag. 39

[21] Il regolamento (UE) 2016/679 ugualmente menzionato all'art. 47 dei regolamenti UE IOP non fa parte dell'acquis di Schengen e non è pertanto vincolante per la Svizzera.

dell'identità. La relativa base giuridica è costituita dall'articolo 110*f* capoverso 4 LStrI e dall'articolo 34 dei regolamenti UE IOP. Un fascicolo di conferma dell'identità contiene i seguenti dati: il tipo di collegamento tra i dati, ossia il collegamento giallo, verde, rosso o bianco (lett. a), il riferimento ai sistemi di informazione Schengen/Dublino in cui sono registrati i dati oggetto del collegamento (lett. b), il numero di identificazione unico che permette di estrarre i dati oggetto del collegamento dai corrispondenti sistemi di informazione Schengen/Dublino (lett. c), l'autorità responsabile della verifica manuale delle identità diverse (lett. d) nonché la data della creazione del collegamento o di un suo aggiornamento (lett. e).

L'*articolo 26 capoverso 2* rinvia all'allegato 2 della presente ordinanza contenente un catalogo dei dati del fascicolo di conferma dell'identità del MID. I relativi diritti di accesso si basano sull'articolo 23 della presente ordinanza che disciplina la verifica manuale di un collegamento giallo nonché sull'articolo 24 della presente ordinanza che definisce l'accesso ai dati provenienti dai collegamenti. Le autorità responsabili della verifica manuale delle identità diverse possono pertanto consultare il fascicolo di conferma dell'identità incluso il collegamento giallo (cfr. art. 110*g* cpv. 2 in combinato disposto con art. 110*f* cpv. 2 e 4 LStrI). Le autorità che hanno accesso ad almeno uno dei sistemi di informazione di cui all'articolo 110*a* LStrI o all'articolo 16*a* LSIP interessati da un collegamento rosso, possono consultare i dati registrati nel fascicolo di conferma dell'identità ai sensi dell'articolo 34 lettere a e b dei regolamenti UE IOP nonché dell'articolo 26 lettere a e b della presente ordinanza (art. 24 cpv. 1 dell'ordinanza N-IOP). Allo stesso modo le autorità che hanno accesso ai sistemi di informazione di cui all'articolo 110*a* LStrI o all'articolo 16*a* LSIP tra i quali esiste un collegamento bianco, possono consultare il fascicolo di conferma dell'identità di cui all'articolo 26 della presente ordinanza (art. 24 cpv. 2 dell'ordinanza N-IOP). Infine le autorità che hanno accesso ai sistemi di informazione di cui all'articolo 110*a* LStrI o all'articolo 16*a* LSIP tra i quali esiste un collegamento verde, possono consultare il fascicolo di conferma dell'identità ai sensi dell'articolo 26 della presente ordinanza, se dalla consultazione è emersa una corrispondenza tra i dati oggetto del collegamento (art. 24 cpv. 3 dell'ordinanza N-IOP). I summenzionati diritti ai dati secondo il capoverso 1 sono illustrati nell'allegato 2.

### Articolo 27

L'*articolo 27* disciplina la conservazione dei dati nel fascicolo di conferma dell'identità. In linea con quanto spiegato riguardo all'sBMS e al CIR (cfr. commenti agli art. 6 e 15), i fascicoli di conferma dell'identità e i relativi dati sono conservati soltanto finché i dati oggetto del collegamento sono conservati nei sistemi di informazione sottostanti. Successivamente sono cancellati dal MID automaticamente. Questa disposizione riprende il contenuto dispositivo dell'articolo 35 dei regolamenti UE IOP.

**Articolo 28**

L'*articolo 28* regolamenta la verbalizzazione dei dati nel MID. Ogni consultazione del MID deve essere indicata all'interno di un verbale. La verbalizzazione va effettuata dalla Confederazione. La competenza specifica incombe all'autorità che ha consultato il sistema di informazione Schengen/Dublino sottostante. Tale obbligo deriva dall'articolo 36 paragrafo 2 dei regolamenti UE IOP. Ciascuno Stato membro conserva pertanto i verbali sulle consultazioni effettuate dalle autorità da esso autorizzate. I verbali garantiscono che i diritti concessi in virtù della sezione 6 della presente ordinanza possano essere effettivamente esercitati dalle persone interessate. Le seguenti informazioni devono essere verbalizzate dall'autorità che ha effettuato la consultazione: l'utente che ha avviato la consultazione, da cui si evince anche l'autorità di appartenenza (lett. a), la finalità dell'accesso dell'utente (lett. b), la data e l'ora della consultazione (lett. c) e il tipo di dati usati per avviare la consultazione (lett. d).

**Sezione 6**

La sezione 6 disciplina i diritti delle persone interessate che sono registrate nei sistemi di informazione Schengen/Dublino e nelle relative componenti.

**Articolo 29**

L'*articolo 29 capoverso 1* disciplina i diritti in materia di informazione, rettifica e cancellazione di dati, il cui esercizio spetta alle persone iscritte nei sistemi di informazione Schengen/Dublino. A tal fine rinvia pertanto alle ordinanze che disciplinano i rispettivi sistemi di informazione. In caso di registrazioni nell'N-SIS la procedura è retta dagli articoli 50 e 51 dell'ordinanza N-SIS (lett. a). Anche per le registrazioni nel C-VIS, nell'EES e nell'ETIAS la procedura è retta dalle ordinanze che regolamentano i rispettivi sistemi di informazione. Poiché le ordinanze relative al VIS, all'EES e all'ETIAS sono attualmente in fase di elaborazione, i rinvii precisi agli articoli saranno inseriti in un secondo momento. Inoltre, dato che il regolamento Eurodac riveduto non è stato ancora recepito, non è possibile per il momento rinviare all'Eurodac.

L'*articolo 29 capoverso 2* precisa che le richieste di informazione, rettifica e cancellazione di collegamenti e dati nel MID, nonché di dati nel CIR devono essere presentate alla SEM. Tale disposizione si fonda sugli articoli 8 e 21 della presente ordinanza che disciplinano la responsabilità per il trattamento dei dati nel CIR e nel MID. Secondo tali disposizioni la SEM è infatti competente per il trattamento dei dati nel CIR. È inoltre responsabile anche per il trattamento dei dati nel MID, nella misura in cui aggiunge o modifica dati nel fascicolo di conferma dell'identità concernenti i sistemi di informazione da essa gestiti. Appare pertanto opportuno designare nell'articolo 29 la SEM come punto di contatto per le richieste di informazione, rettifica e cancellazione di collega-

menti e dati nel MID nonché di dati nel CIR. Si presume infatti che la maggior parte dei collegamenti nel MID riguarderanno *esclusivamente* sistemi di informazioni della SEM (VIS, EES, ETIAS). Nello specifico la richiesta scritta va presentata al servizio centrale di esperti del MID presso la SEM, che sarà creato per offrire sostegno alla verifica manuale dei collegamenti del MID. Se da un suo esame della richiesta emerge che la responsabilità spetta a un'autorità diversa dalla SEM (vale a dire nei casi in cui è interessato l'N-SIS), il servizio centrale di esperti del MID contatta l'autorità in questione. Quest'ultima esamina i motivi della richiesta prima di procedere, se del caso, alla rettifica o alla cancellazione dei collegamenti e dei dati in questione nel MID o nel CIR. La SEM informa in seguito il richiedente (cfr. cpv. 3).

L'*articolo 29 capoverso 3* precisa che la SEM tratta le richieste di cui al capoverso 2 d'intesa con l'autorità competente che ha iscritto o fatto iscrivere i dati in questione. Se il trattamento dei dati nel CIR compete alla SEM (art. 8), quello nel MID incombe alla SEM e a fedpol (art. 21). Se esiste un collegamento del MID con il SIS, la SEM si consulta con fedpol. Altrimenti la consultazione avviene con i servizi interni alla SEM. In questo modo viene garantito che i motivi della registrazione siano sufficientemente noti.

L'*articolo 29 capoverso 4* stabilisce che una persona i cui dati personali sono registrati nel MID può chiedere la rettifica o la cancellazione conformemente all'articolo 48 dei regolamenti UE IOP. La richiesta contiene le informazioni necessarie per identificare le persone interessate (tali informazioni possono essere utilizzate esclusivamente per permettere alla persona interessata di esercitare i propri diritti e devono essere successivamente cancellate senza indugio). La responsabilità per la verifica e, se del caso, la rettifica o la cancellazione delle richieste è affidata all'autorità responsabile per la verifica manuale di un collegamento giallo in virtù dell'articolo 22 della presente ordinanza. Se sono rettificati o cancellati dati, la persona interessata ne viene informata per iscritto. Se l'autorità responsabile per la verifica manuale di un collegamento giallo non ritiene che i dati siano stati registrati in modo errato o illecito, emana una decisione impugnabile in cui enuncia perché non è disponibile a procedere a una rettifica o cancellazione. La decisione deve indicare i rimedi giuridici e può essere impugnata dinanzi a un giudice; sono applicabili i rimedi giuridici ordinari.

### Articolo 30

L'*articolo 30 capoverso 1* statuisce che le autorità cantonali di protezione dei dati e l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) collaborano nell'ambito delle rispettive competenze e coordinano la vigilanza sul trattamento dei dati personali. Tale disposizione si fonda sull'articolo 51 dei regolamenti UE IOP secondo cui le autorità di controllo indipendenti monitorano la legittimità del trattamento dei dati personali effettuato nell'ambito dell'interoperabilità. In Svizzera tale funzione spetta alle autorità cantonali di protezione dei dati e all'IFPDT.

L'*articolo 30 capoverso 2* statuisce che l'IFPDT coopera, nell'esercizio delle proprie funzioni, con il Garante europeo della protezione dei dati, fungendo da referente per quest'ultimo. Tale disposizione si fonda sull'articolo 22 dell'ordinanza OSIU attualmente in fase di elaborazione.

L'*articolo 30 capoverso 3* rimanda per gli ulteriori dettagli all'articolo 51 dei regolamenti UE IOP. In questo modo viene precisato che detti regolamenti costituiscono la base per la vigilanza sul trattamento dei dati. L'IFPDT può pertanto garantire che almeno ogni quattro anni le autorità nazionali competenti svolgono un audit dei trattamenti di dati personali. L'IFPDT è inoltre tenuto a pubblicare ogni anno il numero delle richieste di rettifica, cancellazione o limitazione del trattamento dei dati personali, le conseguenti azioni intraprese e il numero delle rettifiche, cancellazioni e limitazioni del trattamento effettuate in seguito alle richieste degli interessati.

**Sezione 7**

La sezione 7 disciplina la sicurezza dei dati.

**Articolo 31**

L'*articolo 31 capoverso 1* disciplina la sicurezza dei dati. In particolare statuisce che per garantire la sicurezza dei dati si applicano l'ordinanza del 25 novembre 2020 sulla trasformazione digitale e l'informatica (RS *172.010.58*) come pure l'ordinanza del 27 maggio 2020 sui ciber-rischi (RS *120.73*). A tale riguardo occorre rinviare anche all'articolo 42 paragrafi 1 e 4 dei regolamenti UE IOP che disciplina la sicurezza del trattamento dei dati personali.

L'*articolo 31 capoverso 2* intende garantire che le autorità con accesso alle componenti dell'interoperabilità prendano i provvedimenti tecnici e organizzativi necessari conformemente alle disposizioni in materia di protezione dei dati, al fine di impedire l'accesso ai dati alle persone non autorizzate. Questi provvedimenti devono corrispondere alle misure di sicurezza menzionate nell'articolo 42 paragrafo 3 dei regolamenti UE IOP (v. art. 42 par. 2 dei regolamenti UE IOP).

**Sezione 8**

La sezione 8, e nello specifico l'*articolo 32*, disciplina l'entrata in vigore dell'ordinanza. La data dell'entrata in vigore sarà inserita in un secondo momento.

## 3. Futuri adeguamenti di altre ordinanze

### 3.1. Ordinanze che disciplinano i sistemi di informazione Schengen/Dublino

Diverse ordinanze che disciplinano i sistemi di informazione Schengen/Dublino devono essere sottoposte a revisione per via dell'interoperabilità. Ad esempio nell'ordinanza OSIU occorre defi-

nire quali dati possono essere registrati anche nel CIR e indicarne i tempi di cancellazione. L'ordinanza ETIAS va adeguata riguardo ai dati che devono essere registrati anche nel CIR. Quest'ordinanza sarà elaborata prossimamente e dovrebbe entrare in vigore a dicembre 2022. Anche l'ordinanza VIS andrà adeguata in un prossimo futuro, ugualmente in relazione ai dati da registrare anche nel CIR. Infine, il progetto di revisione dell'Eurodac intende rendere questo sistema interoperabile con altri sistemi di informazione. A tal fine sarà elaborata un'ordinanza Eurodac che conterrà tutti gli elementi rilevanti in materia di interoperabilità. Lo sviluppo dell'Eurodac è attualmente parte del patto europeo sulla migrazione e verrà approvato a livello europeo unitamente al patto. Alla fine è stata presa in considerazione anche l'eventualità di stralciare il progetto dal patto sulla migrazione permettendo così un'entrata in vigore anteriore dell'interoperabilità con l'Eurodac. Nelle ordinanze di cui sopra occorre prevedere anche una nuova procedura per l'accesso delle autorità di perseguimento penale ai sistemi EES, VIS e ETIAS in seguito a una consultazione del CIR. Le ordinanze saranno adeguate in modo tale da prevedere entrambe le possibilità di consultazione. La priorità sarà in ogni caso sempre data alla consultazione del CIR. Poiché le ordinanze summenzionate in parte non sono ancora disponibili, al momento non è ancora possibile allestire una lista di tutte le modifiche apportate a tali testi. Tuttavia, si tratta di adeguamenti di minima entità.

### 3.2. Altre ordinanze

Anche altre ordinanze necessitano di essere sottoposte a revisione per via dell'interoperabilità. È previsto infatti un adeguamento dell'articolo 19 capoverso 1 dell'ordinanza SIMIC (RS *142.513*) che consiste nell'eliminare il rinvio all'articolo 111*f* LStrI che, con l'entrata in vigore della nuova struttura della LStrI, introdotta dal decreto federale sull'interoperabilità, viene abrogato (FF *2021* 674). Un'ulteriore modifica riguarda l'ordinanza sull'ammissione, il soggiorno e l'attività lucrativa (OASA, RS *142.201*) il cui articolo 87*a* non dovrà più rinviare all'articolo 111*i* LStrI, bensì all'articolo 109*k* LStrI, introdotto dal decreto federale sull'interoperabilità.

## 4. Ripercussioni finanziarie e sull'effettivo del personale

### 4.1. Ripercussioni sulle finanze e sul personale della Confederazione

L'ordinanza N-IOP non dovrebbe comportare costi supplementari rispetto alle stime enunciate nel messaggio (FF *2020* 7005, in particolare pagg. 7068-7074). Per la Confederazione, il progetto avrà ripercussioni sulle finanze e sul personale sia nella fase di progettazione sia nell'applicazione dei regolamenti UE sull'interoperabilità. L'interoperabilità fa parte del programma del DFGP relativo agli sviluppi di Schengen. I progetti di fedpol e della SEM s'inseriscono all'interno di un credito d'impegno per lo sviluppo dell'acquis di Schengen/Dublino. I costi complessivi per la Confederazione derivanti dai progetti in materia di interoperabilità sono stimati a 21 milioni di franchi per l'intero periodo che va dal 2020 al 2025. Si prevedono costi d'esercizio pari a 0,2 milioni di franchi

nel 2023 e a 2 milioni di franchi ogni anno a partire dal 2024.

Con decisione del 12 maggio 2021, il Consiglio federale ha preso atto del fabbisogno supplementare in termini di personale derivante dall'interoperabilità fino al 2023. Il fabbisogno per il 2022 è stato approvato dal Consiglio federale, con decisione del 23 giugno 2021, nel quadro della valutazione globale 2021 delle risorse nel settore del personale. Il fabbisogno per il 2023 sarà nuovamente esaminato dal DFGP nell'ambito dell'allestimento del preventivo 2023. Il fabbisogno supplementare di personale attualmente previsto a partire dal 2024 sarà oggetto di una richiesta che sarà sottoposta al Consiglio federale in un secondo momento.

### 4.2. Ripercussioni sulle finanze e sul personale dei Cantoni

Le autorità cantonali di migrazione e di polizia potranno avvalersi dell'interoperabilità per lo svolgimento delle loro attività. Ciò richiederà adeguamenti sul piano tecnico e dei processi ai sistemi cantonali di consultazione. Attualmente Confederazione e Cantoni stanno lavorando a stretto contatto per individuare tali modifiche. Con l'istituzione del servizio centrale di esperti del MID, la Confederazione sgraverà i Cantoni dalla verifica delle identità. Il fabbisogno supplementare di personale è indicato dettagliatamente all'interno del messaggio IOP (FF *2020* 7005, in particolare pag. 7073).

## 5. Aspetti giuridici

### 5.1. Costituzionalità

Gli scambi di note tra la Svizzera e l'UE concernenti il recepimento dei regolamenti UE sull'interoperabilità sono retti dall'articolo 54 capoverso 1 Cost. e sono stati sottoposti per approvazione all'Assemblea federale[22].

Il presente progetto tiene conto dei requisiti costituzionali e assicura in particolare che siano garantite le garanzie procedurali (cfr. sezione 6). Alla luce delle basi giuridiche previste come pure dei principi, sanciti per legge, in materia di protezione e sicurezza dei dati, le ingerenze nei diritti fondamentali già previste a livello di legge appaiono proporzionate rispetto allo scopo perseguito (art. 36 cpv. 1-3 Cost.).

### 5.2. Compatibilità con altri impegni internazionali della Svizzera

Le modifiche dell'ordinanza sono conformi al diritto internazionale. Con il recepimento dei due sviluppi dell'acquis di Schengen, la Svizzera adempie i propri impegni derivanti dall'AAS. Contri-

[22] Messaggio IOP, FF **2020** 7005, in particolare pag. 7075 seg.

buisce inoltre all'applicazione uniforme dei sistemi d'informazione Schengen/Dublino. Il recepimento dei due regolamenti UE e le modifiche legislative che ne derivano sono pertanto compatibili con gli impegni internazionali della Svizzera.

### 5.3. Forma dell'atto

Con il presente progetto sono apportate le modifiche necessarie a livello di ordinanza ai fini dell'attuazione dell'interoperabilità. Si tratta in primo luogo di disposizioni necessarie ad attuare le modifiche di legge. Determinate disposizioni dei regolamenti UE IOP richiedono inoltre una concretizzazione a livello di ordinanza. Gli atti giuridici terziari finora notificati (decisioni di esecuzione) in materia di interoperabilità necessitano infine di essere attuati. Da queste considerazioni nasce dunque la necessità di elaborare l'ordinanza sull'interoperabilità tra i sistemi di informazione Schengen/Dublino, la cosiddetta ordinanza N-IOP.

## 6. Protezione dei dati

In seguito all'introduzione delle nuove componenti centrali, che influiscono su tutti i sistemi d'informazione Schengen/Dublino, sono stati apportati gli adeguamenti necessari a livello di legge, in particolare in materia di protezione dei dati (cfr. capitoli 14, 14*a*, 14*b* e 14*c* LStrI). Ulteriori disposizioni in materia di protezione dei dati sono presenti anche nel presente progetto (cfr. sezioni 6 e 7).