2025/2447

5.12.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/2447 DELLA COMMISSIONE

del 4 dicembre 2025

recante modalità di applicazione del regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio per quanto riguarda le specifiche tecniche, le misure tecniche e gli altri requisiti tecnici per l'istituzione e l'uso del sistema informatico decentrato per il trattamento e la comunicazione sicuri delle informazioni

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, de 14 de novembre 2018 che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio ([1]), in particolare l'articolo 22 *bis*, paragrafo 3, e l'articolo 22 *ter*, paragrafo 1, lettere a), b), c) e d),

considerando quanto segue:

(1) Il regolamento (UE) 2018/1727 stabilisce il quadro per la nuova infrastruttura digitale interna di Eurojust e l'istituzione di un sistema decentrato per la comunicazione digitale sicura tra le autorità nazionali competenti degli Stati membri ed Eurojust.

(2) La comunicazione digitale sicura deve avvenire attraverso il sistema informatico decentrato. Per istituire il sistema informatico decentrato è necessario stabilire specifiche tecniche che definiscano i metodi e i protocolli di comunicazione e misure tecniche che garantiscano le norme minime di sicurezza delle informazioni e la sicurezza, e definire gli obiettivi minimi di disponibilità per l'attuazione di tale sistema.

(3) Conformemente all'articolo 22 *bis*, paragrafo 1, del regolamento (UE) 2018/1727, il sistema informatico decentrato comprende i sistemi informatici degli Stati membri e di Eurojust, così come i punti di accesso e-CODEX interoperabili attraverso i quali tali sistemi sono interconnessi. Le specifiche tecniche e gli altri requisiti tecnici del sistema informatico decentrato di cui al presente regolamento dovrebbero tenere conto di tale quadro.

(4) I punti di accesso del sistema informatico decentrato dovrebbero basarsi su punti di accesso e-CODEX autorizzati quali definiti all'articolo 3, punto 3), del regolamento (UE) 2022/850 del Parlamento europeo e del Consiglio ([2]).

(5) Il sistema informatico decentrato è attuato nell'ambito di un più ampio sistema informatico decentrato basato su e-CODEX, denominato *Justice Digital EXchange system* (JUDEX). È pertanto necessario garantire uno scambio di informazioni efficace sugli sviluppi orizzontali.

(6) Conformemente all'articolo 22 *bis*, paragrafo 4, del regolamento (UE) 2018/1727, gli Stati membri possono scegliere di utilizzare il software di implementazione di riferimento sviluppato dalla Commissione come loro sistema back-end invece di un sistema informatico nazionale. Al fine di garantire l'interoperabilità, i sistemi informatici nazionali e il software di implementazione di riferimento dovrebbero essere soggetti alle stesse specifiche tecniche e agli stessi requisiti tecnici.

(7) I dati relativi ai reati di terrorismo e alle forme gravi di criminalità organizzata dovrebbero essere trasmessi in modo strutturato per migliorare la qualità e la rilevanza delle informazioni e per garantire che le informazioni possano essere integrate in modo più efficiente nel sistema automatico di gestione dei fascicoli di Eurojust e sottoposte a un migliore controllo incrociato con quelle già conservate in tale sistema. È opportuno definire il formato e le norme tecniche per la trasmissione dei dati relativi alle impronte digitali e le fotografie che possono essere inviati a Eurojust al fine di identificare le persone oggetto di procedimenti penali connessi a reati di terrorismo.

([1]) (GU L 295 del 21.11.2018, pag. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj).

([2]) Regolamento (UE) 2022/850 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo a un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726 (GU L 150 dell'1.6.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust agevola e sostiene l'emissione e l'esecuzione delle richieste di cooperazione giudiziaria, anche con riferimento a richieste e decisioni basate sugli strumenti che attuano il principio del riconoscimento reciproco. Le autorità nazionali competenti dovrebbero poter chiedere assistenza e coordinamento a Eurojust tramite il sistema informatico decentrato.

(9) Al fine di garantire efficienza e coerenza, è importante che le specifiche tecniche da stabilire nel quadro del regolamento (UE) 2018/1727 siano compatibili con le specifiche tecniche stabilite a norma dei regolamenti (UE) 2023/2844 ([3]), (UE) 2023/1543 ([4]) e (UE) 2024/3011 ([5]) del Parlamento europeo e del Consiglio, nonché con le future misure di digitalizzazione attinenti al mandato di Eurojust per aiutare le autorità nazionali competenti.

(10) Qualsiasi altra comunicazione tra Eurojust e le autorità nazionali competenti, come la comunicazione di informazioni relative ai risultati del trattamento delle informazioni e all'esistenza di collegamenti con casi già registrati nel sistema automatico di gestione dei fascicoli a norma dell'articolo 22 del regolamento (UE) 2018/1727 quando Eurojust agisce di propria iniziativa, o di informazioni trasmesse a Eurojust al fine di preservare, analizzare e conservare prove relative a genocidio, crimini contro l'umanità, crimini di guerra e reati connessi conformemente all'articolo 4, paragrafo 1, lettera j), di tale regolamento, dovrebbe essere consentita anche tramite il sistema informatico decentrato.

(11) Per garantire che il presente regolamento tenga conto delle esigenze operative di Eurojust, quest'ultima è stata consultata conformemente all'articolo 22 *bis*, paragrafo 3, del regolamento (UE) 2018/1727.

(12) A norma dell'articolo 4 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, con lettera del 9 settembre 2019, l'intenzione di accettare il regolamento (UE) 2018/1727 e di esserne vincolata. Tale partecipazione è stata confermata con decisione (UE) 2019/2006 della Commissione ([6]). Il regolamento (UE) 2023/2131 del Parlamento europeo e del Consiglio ([7]) ha modificato il regolamento (UE) 2018/1727 per consentire l'istituzione di canali di comunicazione digitale sicuri tra Eurojust e le autorità nazionali competenti e costituisce la base giuridica del presente regolamento. Non avendo notificato l'intenzione di partecipare all'adozione e all'applicazione del regolamento (UE) 2023/2131 e non avendo notificato l'intenzione di accettare tale regolamento ed esserne vincolata, l'Irlanda non è vincolata dal regolamento (UE) 2023/2131 né è soggetta alla sua applicazione, a norma degli articoli 1 e 2 e dell'articolo 4 *bis*, paragrafo 1, del protocollo n. 21. L'Irlanda non partecipa quindi all'adozione del presente regolamento.

(13) 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 ha partecipato all'adozione del regolamento (UE) 2018/1727. La Danimarca non è pertanto vincolata dal presente regolamento né è soggetta alla sua applicazione.

([3]) Regolamento (UE) 2023/2844 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, sulla digitalizzazione della cooperazione giudiziaria e dell'accesso alla giustizia in materia civile, commerciale e penale a livello transfrontaliero e che modifica taluni atti nel settore della cooperazione giudiziaria (GU L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali (GU L 191 del 28.7.2023, pag. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Regolamento (UE) 2024/3011 del Parlamento europeo e del Consiglio, del 27 novembre 2024, sul trasferimento dei procedimenti penali (GU L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Decisione (UE) 2019/2006 della Commissione, del 29 novembre 2019, relativa alla partecipazione dell'Irlanda al regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) (GU L 310 del 2.12.2019, pag. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Regolamento (UE) 2023/2131 del Parlamento europeo e del Consiglio, del 4 ottobre 2023, che modifica il regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio e la decisione 2005/671/GAI del Consiglio, per quanto riguarda lo scambio digitale di informazioni nei casi di terrorismo (GU L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([8]), il Garante europeo della protezione dei dati è stato consultato e ha espresso un parere il 21 ottobre 2025.

(15) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 22 *quater* del regolamento (UE) 2018/1727,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Specifiche tecniche del sistema informatico decentrato

Le specifiche tecniche, le misure tecniche e gli obiettivi del sistema informatico decentrato di cui all'articolo 22 *ter*, paragrafo 1, lettere a), b), c) e d), del regolamento (UE) 2018/1727 figurano nell'allegato I del presente regolamento.

Articolo 2

Standard procedurali digitali

Gli standard procedurali digitali applicabili alla comunicazione elettronica tramite il sistema informatico decentrato di cui all'articolo 22 *bis*, paragrafo 3, del regolamento (UE) 2018/1727 sono stabiliti nell'allegato II del presente regolamento.

Articolo 3

Specifiche tecniche per la trasmissione di impronte digitali e fotografie

Le specifiche tecniche e il formato per la trasmissione di impronte digitali e fotografie di cui all'articolo 22 *bis*, paragrafo 3, del regolamento (UE) 2018/1727 sono stabiliti nell'allegato III del presente regolamento.

Articolo 4

Entrata in vigore

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 4 dicembre 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

([8]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ALLEGATO I

SPECIFICHE TECNICHE, MISURE TECNICHE E OBIETTIVI DEL SISTEMA INFORMATICO DECENTRATO

1. **Introduzione e oggetto**

Il presente allegato stabilisce le specifiche tecniche, le misure tecniche e gli obiettivi del sistema informatico decentrato per lo scambio di informazioni di cui al regolamento (UE) 2018/1727.

La natura decentrata del sistema informatico consente lo scambio diretto e sicuro dei dati tra le autorità nazionali competenti ed Eurojust.

2. **Definizioni**

Ai fini del presente allegato si applicano le definizioni seguenti:

2.1. «Protocollo di trasferimento per ipertesti sicuro» (*Hypertext Transfer Protocol Secure*) o «HTTPS»: canali di connessione protetta e di comunicazione criptata;

2.2. «non disconoscibilità dell'origine»: le misure che forniscono la prova dell'integrità e la prova dell'origine dei dati attraverso metodi come la certificazione digitale, l'infrastruttura a chiave pubblica, le firme digitali e i sigilli elettronici;

2.3. «non disconoscibilità del ricevimento»: le misure che forniscono al mittente la prova che il destinatario previsto ha ricevuto i dati, attraverso metodi come la certificazione digitale, l'infrastruttura a chiave pubblica, la firma digitale e i sigilli elettronici;

2.4. «*Simple Object Access Protocol*» (SOAP): secondo gli standard del World Wide Web Consortium, protocollo per la trasmissione di messaggi per lo scambio di informazioni strutturate nell'attuazione dei servizi web in reti di computer;

2.5. «trasferimento di stato rappresentativo» (*Representational State Transfer*, REST): uno stile architettonico per la progettazione di applicazioni in rete, basato su un modello di comunicazione client-server senza stato, e che utilizza metodi standard per effettuare operazioni sulle risorse, generalmente rappresentati in formati strutturati;

2.6. «servizio web»: applicazione informatica progettata per supportare l'interazione e l'interoperabilità tra macchine all'interno di una rete, e che ha un'interfaccia descritta in un formato elaborabile automaticamente;

2.7. «scambio di dati»: lo scambio di messaggi e documenti attraverso il sistema informatico decentrato;

2.8. «e-CODEX»: il sistema e-CODEX di cui all'articolo 3, punto 1), del regolamento (UE) 2022/850;

2.9. «vocabolario di base dell'UE della giustizia elettronica»: il vocabolario di base dell'UE della giustizia elettronica quale definito al punto 4) dell'allegato del regolamento (UE) 2022/850;

2.10. «ebMS»: il servizio di messaggistica ebXML, un protocollo di messaggistica sviluppato nell'ambito di OASIS che consente lo scambio sicuro, affidabile e interoperabile di documenti commerciali elettronici utilizzando SOAP. Sostiene l'integrazione interaziendale in diversi sistemi;

2.11. «AS4»: dichiarazione di applicabilità 4 (*Applicability Statement* 4), uno standard OASIS profilo di ebMS 3.0; semplifica la messaggistica interaziendale sicura e interoperabile utilizzando standard aperti quali SOAP e WS-Security;

2.12. «tempo massimo di ripristino»: il tempo massimo accettabile per ripristinare il servizio dopo un incidente;

2.13. «punto di ripristino prefissato»: la quantità massima accettabile di perdita di dati in caso di guasto.

3. **Metodi di comunicazione per via elettronica**

3.1. Ai fini dello scambio di messaggi e documenti, il sistema informatico decentrato utilizza metodi di comunicazione basati sui servizi, come servizi web o altri componenti e soluzioni software riutilizzabili.

3.2. Nello specifico, il sistema informatico decentrato comporta la comunicazione attraverso i punti di accesso e-CODEX, come stabilito all'articolo 5, paragrafo 2, del regolamento (UE) 2022/850. Pertanto, al fine di garantire uno scambio transfrontaliero di dati efficace e interoperabile, il sistema informatico decentrato supporta la comunicazione attraverso il sistema e-CODEX.

4. **Protocolli di comunicazione**

4.1. Il sistema informatico decentrato utilizza protocolli Internet sicuri per:

a) la comunicazione tra le autorità competenti ed Eurojust all'interno del sistema informatico decentrato;

b) la comunicazione con la banca dati dell'autorità competente/degli organi giurisdizionali a norma del punto 7.1.

4.2. Per la definizione e la trasmissione di dati e metadati strutturati, i componenti del sistema informatico decentrato si basano su standard e protocolli di settore completi e ampiamente accettati, quali SOAP e REST.

4.3. Per i protocolli di trasporto e messaggistica, il sistema informatico decentrato si basa su protocolli sicuri, basati su standard, quali:

a) profilo AS4 per lo scambio transfrontaliero di dati, che garantisce una messaggistica sicura e affidabile con cifratura e non disconoscibilità;

b) HTTPS/RESTful API per la comunicazione che supportano i formati JSON e XML;

c) SOAP per le interazioni ad alta affidabilità, che integra WS-Security per l'autenticazione e la cifratura.

4.4. Ai fini di uno scambio di dati fluido e interoperabile, i protocolli di comunicazione utilizzati dal sistema informatico decentrato sono conformi alle pertinenti norme di interoperabilità.

4.5. Se del caso, gli schemi XML si avvalgono di standard o vocabolari pertinenti, necessari per la corretta convalida degli elementi e dei tipi definiti in tale schema. Tali standard o vocabolari possono comprendere:

a) il vocabolario di base dell'UE della giustizia elettronica;

b) tipi di dati non qualificati;

c) un elenco di codici per i codici linguistici dell'Unione europea.

4.6. Per i protocolli di sicurezza e autenticazione, il sistema informatico decentrato si basa su protocolli sicuri, basati su standard, quali:

a) TLS (*Transport Layer Security* - Sicurezza del livello di trasporto) per le comunicazioni criptate e autenticate attraverso le reti, che supporta l'autenticazione reciproca tramite certificati digitali X.509;

b) OAuth/OpenID Connect (OIDC) per una procedura di autenticazione e autorizzazione sicura;

c) infrastruttura a chiave pubblica (*Public Key Infrastructure*, PKI) e firme digitali per lo scambio sicuro delle chiavi e la verifica dell'integrità dei messaggi, utilizzando certificati digitali (X.509) rilasciati da autorità di certificazione fidate.

5. **Obiettivi in materia di sicurezza delle informazioni e pertinenti misure tecniche**

5.1. Per lo scambio di informazioni attraverso il sistema informatico decentrato, le misure tecniche per garantire le norme minime di sicurezza informatica includono:

a) misure atte a garantire la riservatezza delle informazioni, anche con il ricorso a canali protetti di comunicazione;

b) misure atte a garantire l'integrità dei dati a riposo e in transito;

c) misure atte a garantire la non disconoscibilità dell'origine del mittente delle informazioni in seno al sistema informatico decentrato e la non disconoscibilità del ricevimento delle informazioni;

d) misure atte a garantire che gli episodi attinenti alla sicurezza vengano registrati conformemente alle raccomandazioni internazionali riconosciute in materia di norme di sicurezza informatica ([1]);

e) misure atte a garantire l'autenticazione e l'autorizzazione degli utenti e misure di verifica dell'identità dei sistemi connessi al sistema informatico decentrato.

5.2. I componenti del sistema informatico decentrato garantiscono la comunicazione e la trasmissione dei dati sicure utilizzando la cifratura, l'infrastruttura a chiave pubblica con certificati digitali per l'autenticazione e lo scambio sicuro delle chiavi e protocolli di messaggistica sicuri quali AS4 (ebMS), RESTful API e SOAP, al fine di mantenere la riservatezza e l'integrità dei messaggi.

5.3. Se viene impiegato il protocollo TLS nel contesto del sistema informatico decentrato, si utilizza l'ultima versione stabile o, in mancanza di questa, una versione senza vulnerabilità note in materia di sicurezza. Sono consentite solo chiavi di lunghezza tale da garantire un livello adeguato di sicurezza crittografica e non sono utilizzate suite di cifratura notoriamente non sicure o obsolete.

5.4. Nella misura del possibile, i certificati digitali PKI utilizzati ai fini del funzionamento del sistema informatico decentrato sono rilasciati dalle autorità di certificazione riconosciute come prestatori di servizi fiduciari qualificati a norma del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([2]). Sono attuate misure per garantire che tali certificati siano utilizzati esclusivamente per i fini previsti, al livello di fiducia richiesto e nel rispetto dei requisiti applicabili di cui al regolamento (UE) n. 910/2014.

5.5. I componenti del sistema informatico decentrato sono sviluppati conformemente al principio della protezione dei dati fin dalla progettazione e per impostazione predefinita, e vengono attuate misure amministrative, organizzative e tecniche adeguate per garantire un livello elevato di cibersicurezza.

5.6. La Commissione progetta, sviluppa e mantiene il software di implementazione di riferimento in conformità dei requisiti e dei principi in materia di protezione dei dati stabiliti dal regolamento (UE) 2018/1725. Il software di implementazione di riferimento fornito dalla Commissione consente agli Stati membri di adempiere ai loro obblighi a norma rispettivamente del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([3]) e della direttiva (UE) 2016/680, a seconda dei casi.

([1]) Fatta salva la registrazione a fini di sicurezza, i meccanismi di registrazione utilizzati dai componenti del sistema informatico decentrato consentono, a seconda dei casi, di garantire la conformità ai requisiti di cui all'articolo 88 del regolamento (UE) 2018/1725 e, se del caso, all'articolo 25 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 Consiglio (GU L 119 del 4.5.2016, pag. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Gli Stati membri che utilizzano un sistema back-end nazionale diverso dal software di implementazione di riferimento attuano le misure necessarie per garantirne la conformità ai requisiti del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680, a seconda dei casi.

5.8. Eurojust attua le misure necessarie per garantire che il suo sistema back-end, o un'istanza del software di implementazione di riferimento che utilizza, sia conforme ai requisiti dei regolamenti (UE) 2018/1725 e (UE) 2018/1727.

5.9. Gli Stati membri ed Eurojust istituiscono meccanismi solidi per il rilevamento delle minacce e la risposta agli incidenti, al fine di garantire tempestivamente l'individuazione e la mitigazione degli incidenti di sicurezza e il successivo ripristino, conformemente alle rispettive politiche in materia, per i sistemi informatici soggetti alla loro competenza che fanno parte del sistema informatico decentrato.

6. **Obiettivi minimi di disponibilità**

6.1. Eurojust e gli Stati membri garantiscono 24 ore su 24 e 7 giorni su 7 la disponibilità dei componenti del sistema informatico decentrato soggetti alla loro competenza, con l'obiettivo di un tasso di disponibilità tecnica almeno del 98 % su base annua, esclusa la manutenzione programmata.

6.2. La Commissione garantisce 24 ore su 24 e 7 giorni su 7 la disponibilità della banca dati degli organi giurisdizionali, con l'obiettivo di un tasso di disponibilità tecnica superiore al 99 % su base annua, esclusa la manutenzione programmata.

6.3. Nella misura del possibile, durante i giorni lavorativi, le operazioni di manutenzione sono programmate tra le ore 20:00 e le ore 7:00 CET.

6.4. Gli Stati membri notificano alla Commissione, a Eurojust e agli altri Stati membri le attività di manutenzione come segue:

a) con un anticipo di 5 giorni lavorativi per le operazioni di manutenzione che possono comportare un periodo di indisponibilità fino a 4 ore;

b) con un anticipo di 10 giorni lavorativi per le operazioni di manutenzione che possono comportare un periodo di indisponibilità compreso tra 4 e 12 ore;

c) con un anticipo di 30 giorni lavorativi per le operazioni di manutenzione che possono comportare un periodo di indisponibilità superiore a 12 ore.

6.5. Qualora gli Stati membri abbiano stabilito periodi di manutenzione regolari, comunicano alla Commissione, a Eurojust e agli altri Stati membri l'ora e il giorno/i giorni in cui sono programmati tali periodi fissi regolari. In deroga agli obblighi di cui alla prima frase, in caso di indisponibilità dei componenti del sistema informatico decentrato soggetti alla loro competenza durante tale periodo fisso regolare, gli Stati membri non sono tenuti a comunicare ogni volta alla Commissione tale indisponibilità.

6.6. In caso di guasto tecnico imprevisto di un componente del sistema informatico decentrato soggetto alla loro competenza, gli Stati membri ne informano immediatamente la Commissione e gli altri Stati membri e, se noto, indicano il previsto periodo di ripristino.

6.7. Eurojust notifica alla Commissione e agli Stati membri le attività di manutenzione come segue:

a) con un anticipo di 5 giorni lavorativi per le operazioni di manutenzione che possono comportare un periodo di indisponibilità fino a 4 ore;

b) con un anticipo di 10 giorni lavorativi per le operazioni di manutenzione che possono comportare un periodo di indisponibilità compreso tra 4 e 12 ore;

c) con un anticipo di 30 giorni lavorativi per le operazioni di manutenzione che possono comportare un periodo di indisponibilità superiore a 12 ore.

6.8. Qualora Eurojust abbia stabilito periodi di manutenzione regolari, essa comunica alla Commissione e agli Stati membri l'ora e il giorno/i giorni in cui sono programmati tali periodi fissi regolari. In deroga agli obblighi di cui alla prima frase, in caso di indisponibilità dei componenti del sistema informatico decentrato soggetti alla sua competenza durante tale periodo fisso regolare, Eurojust non è tenuta a comunicare ogni volta alla Commissione tale indisponibilità.

6.9. In caso di guasto tecnico imprevisto di un componente del sistema informatico decentrato soggetto alla sua competenza, Eurojust ne informa immediatamente la Commissione e gli Stati membri e, se noto, indica il previsto periodo di ripristino.

6.10. In caso di guasto tecnico imprevisto della banca dati delle autorità competenti/degli organi giurisdizionali, la Commissione informa senza indugio Eurojust e gli Stati membri di tale indisponibilità e, se noto, del previsto periodo di ripristino.

6.11. In caso di interruzione del servizio, gli Stati membri ed Eurojust garantiscono un rapido ripristino del servizio e una perdita minima di dati, conformemente al tempo massimo di ripristino e al punto di ripristino prefissato.

6.12. Gli Stati membri ed Eurojust attuano misure adeguate per conseguire gli obiettivi di disponibilità sopra indicati e stabiliscono procedure per rispondere efficacemente agli incidenti.

7. **Banca dati delle autorità competenti/degli organi giurisdizionali**

7.1. A norma dell'articolo 22 *bis* del regolamento (UE) 2018/1727, la comunicazione tra le autorità nazionali competenti ed Eurojust ha luogo tramite il sistema informatico decentrato. Considerando gli obblighi di scambio di informazioni tra le autorità nazionali competenti ed Eurojust a norma degli articoli 21, 21 *bis* e 22, ma anche il ruolo di Eurojust nell'agevolare e sostenere l'emissione e l'esecuzione delle richieste di assistenza giudiziaria o di riconoscimento reciproco a norma dell'articolo 8, paragrafo 1, del regolamento (UE) 2018/1727, le autorità competenti coinvolte devono essere chiaramente identificabili quando utilizzano il sistema informatico decentrato. È pertanto essenziale istituire una banca dati accreditata delle informazioni su tali autorità ai fini del sistema informatico decentrato.

7.2. Tale banca dati delle autorità competenti/degli organi giurisdizionali (*Competent authorities/Court database*, CDB) contiene le informazioni seguenti in un formato strutturato:

a) ai fini dell'articolo 8, paragrafi 1, 3 e 4, dell'articolo 21, dell'articolo 21 *bis* e dell'articolo 22 del regolamento (UE) 2018/1727, le informazioni sulle autorità nazionali competenti, compresi i corrispondenti nazionali di cui all'articolo 20 di tale regolamento, nonché sui membri nazionali conformemente all'articolo 7 ([4]) di tale regolamento;

b) se del caso, le informazioni necessarie per determinare le aree geografiche o essenziali di competenza delle autorità competenti, o altri criteri pertinenti necessari per stabilirne la competenza;

c) informazioni necessarie per il corretto instradamento tecnico dei messaggi all'interno del sistema informatico decentrato.

7.3. La Commissione è responsabile dello sviluppo, della manutenzione, del funzionamento e del supporto della CDB.

7.4. La CDB consente agli Stati membri e a Eurojust di aggiornare le informazioni ivi contenute e alle autorità nazionali competenti e ai membri nazionali che partecipano al sistema informatico decentrato di accedere programmaticamente alle informazioni ivi contenute e di recuperarle.

7.5. L'accesso alla CDB è possibile attraverso un protocollo comune di comunicazione, indipendentemente dal fatto che le autorità competenti collegate al sistema informatico decentrato utilizzino un sistema back-end nazionale o un'istanza del software di implementazione di riferimento.

7.6. Gli Stati membri provvedono affinché le informazioni sulle loro autorità competenti di cui al punto 7.2 contenute nella banca dati delle autorità competenti/degli organi giurisdizionali siano complete, esatte e tenute aggiornate.

([4]) Ciò non pregiudica la delega di poteri dal membro nazionale al suo aggiunto, ad altro personale dell'ufficio nazionale o al personale autorizzato di Eurojust.

ALLEGATO II

STANDARD PROCEDURALI DIGITALI

L'articolo 3, punto 9), del regolamento (UE) 2022/850 definisce gli standard procedurali digitali come le specifiche tecniche per i modelli di processo operativo e per i modelli preesistenti di dati che definiscono la struttura elettronica dei dati scambiati attraverso il sistema e-CODEX.

Il presente allegato stabilisce le specifiche tecniche per i modelli di processo operativo e per i modelli preesistenti di dati.

1. **Specifiche tecniche per i modelli di processo operativo a norma del regolamento (UE) 2018/1727**

Le specifiche tecniche per i modelli di processo operativo sono illustrate ai punti da 1.1 a 1.5. Definiscono gli aspetti fondamentali necessari per consentire la comunicazione elettronica ai fini del regolamento (UE) 2018/1727 tramite il sistema informatico decentrato.

Tale sistema consente lo scambio di informazioni solo tra le autorità nazionali competenti di uno Stato membro e il membro nazionale di tale Stato membro.

1.1. *Scambio di informazioni relative al registro giudiziario europeo antiterrorismo (CTR) – articolo 21 bis del regolamento (UE) 2018/1727*

1.1.1. Modello per trasmettere i dati CTR:

l'autorità nazionale competente trasmette al membro nazionale i dati sui procedimenti per terrorismo destinati al CTR.

1.1.2. Modello per ricevere i dati CTR:

il membro nazionale riceve i dati CTR.

1.1.3. Modello per richiedere il consenso:

il membro nazionale chiede il consenso della propria autorità nazionale competente.

1.1.4. Modello per ricevere la richiesta del consenso:

l'autorità nazionale competente riceve la richiesta del consenso.

1.1.5. Modello per inviare una risposta alla richiesta del consenso:

l'autorità nazionale competente invia una risposta alla richiesta di consenso.

1.1.6. Modello per ricevere la risposta alla richiesta del consenso:

il membro nazionale riceve la risposta alla richiesta del consenso.

1.1.7. Modello per comunicare un collegamento:

il membro nazionale informa l'autorità nazionale competente in merito al collegamento con un altro caso.

1.1.8. Modello per aggiornare i dati CTR:

l'autorità nazionale competente trasmette al rispettivo membro nazionale i dati che devono essere aggiornati o cancellati.

1.1.9. Modello per ricevere i dati CTR aggiornati:

il membro nazionale riceve i dati CTR che devono essere aggiornati o cancellati.

1.2. *Scambio di informazioni relative a reati gravi – articolo 21 del regolamento (UE) 2018/1727*

1.2.1. Modello per trasmettere i dati sulle forme gravi di criminalità transfrontaliera:

l'autorità nazionale competente trasmette a Eurojust i dati relativi alle forme gravi di criminalità transfrontaliera.

1.2.2. Modello per ricevere i dati sulle forme gravi di criminalità transfrontaliera:

il membro nazionale riceve i dati relativi alle forme gravi di criminalità transfrontaliera.

1.2.3. Modello per richiedere il consenso:

il membro nazionale chiede il consenso della propria autorità nazionale competente.

1.2.4. Modello per ricevere la richiesta del consenso:

l'autorità nazionale competente riceve la richiesta del consenso.

1.2.5. Modello per inviare una risposta alla richiesta del consenso:

l'autorità nazionale competente invia una risposta alla richiesta di consenso.

1.2.6. Modello per ricevere la risposta alla richiesta del consenso:

il membro nazionale riceve la risposta alla richiesta del consenso.

1.2.7. Modello per comunicare un collegamento:

il membro nazionale informa l'autorità nazionale competente in merito al collegamento con un altro caso.

1.2.8. Modello per aggiornare i dati sulle forme gravi di criminalità transfrontaliera:

l'autorità nazionale competente trasmette al rispettivo membro nazionale i dati che devono essere aggiornati o cancellati.

1.2.9. Modello per ricevere i dati aggiornati sulle forme gravi di criminalità transfrontaliera:

il membro nazionale riceve i dati sulle forme gravi di criminalità transfrontaliera che devono essere aggiornati o cancellati.

1.3. *Scambio di informazioni generali*

1.3.1. Modello per inviare informazioni:

il membro nazionale invia informazioni all'autorità nazionale competente o viceversa.

1.3.2. Modello per ricevere informazioni:

l'autorità nazionale competente o il membro nazionale ricevono le informazioni.

1.3.3. Modello per rispondere alle informazioni:

l'autorità nazionale competente risponde alle informazioni ricevute dal membro nazionale o viceversa.

1.3.4. Modello per ricevere la risposta:

il membro nazionale riceve la risposta dall'autorità nazionale competente.

1.3.5. Modello per inviare informazioni:

l'autorità nazionale competente invia informazioni al membro nazionale.

1.3.6. Modello per ricevere informazioni:

il membro nazionale riceve le informazioni.

1.3.7. Modello per rispondere alle informazioni:

il membro nazionale risponde alle informazioni ricevute dall'autorità nazionale competente.

1.3.8. Modello per ricevere la risposta:

l'autorità nazionale competente riceve la risposta dal membro nazionale.

1.4. *Ruolo di agevolazione e sostegno - articolo 8, paragrafo 1, del regolamento (UE) 2018/1727*

Nota: Se i modelli per l'agevolazione e il sostegno di cui al punto 1.5 comportano lo scambio di modelli stabiliti da atti giuridici dell'Unione nel settore della cooperazione giudiziaria in materia penale, i modelli utilizzano, se disponibili, le pertinenti rappresentazioni di dati strutturati e gli schemi XML sviluppati per tali atti, ad esempio quelli istituiti ai fini del regolamento di esecuzione (UE) 2023/2844 o di altri strumenti pertinenti.

1.5. *Modello per richiedere agevolazione o sostegno*

1.5.1. Modello per trasmettere la richiesta di agevolazione o sostegno:

l'autorità nazionale competente trasmette una richiesta di agevolazione o una richiesta di sostegno al rispettivo membro nazionale.

1.5.2. Modello per ricevere la richiesta di agevolazione o sostegno:

il membro nazionale riceve la richiesta di agevolazione o sostegno e la inoltra al membro nazionale dello Stato membro richiesto al di fuori del sistema JUDEX.

1.5.3. Modello per inoltrare la richiesta di agevolazione o sostegno all'autorità nazionale competente:

il membro nazionale dello Stato membro richiesto invia la richiesta alla rispettiva autorità nazionale competente.

1.5.4. Modello per ricevere la richiesta di agevolazione o sostegno:

l'autorità nazionale competente riceve la richiesta di agevolazione o sostegno.

1.5.5. Modello per rispondere alla richiesta di agevolazione o sostegno:

l'autorità nazionale competente invia una risposta o informazioni relative alla richiesta al membro nazionale dello Stato membro richiesto.

1.5.6. Modello per ricevere la risposta alla richiesta di agevolazione o sostegno:

il membro nazionale riceve la risposta o le informazioni relative alla richiesta di agevolazione o sostegno dall'autorità nazionale competente e le condivide con il membro nazionale dello Stato membro richiesto al di fuori del sistema JUDEX.

1.5.7. Modello per rispondere alla richiesta di agevolazione o sostegno:

il membro nazionale dello Stato membro richiedente risponde o condivide le informazioni relative alla richiesta di agevolazione o sostegno dell'autorità nazionale competente.

1.5.8. Modello per ricevere la risposta:

l'autorità nazionale competente riceve la risposta o le informazioni relative alla richiesta di agevolazione o sostegno.

2. **Specifiche tecniche per gli schemi dei dati**

Le specifiche tecniche che devono servire da base per lo sviluppo di *XML Schema Definition* (XSD) per la digitalizzazione del regolamento (UE) 2018/1727 sono stabilite ai punti 2.1 e 2.2 del presente allegato. Tali specifiche definiscono i componenti fondamentali e qualsiasi altra informazione per fornire una descrizione completa per la produzione di tali schemi.

La descrizione deve essere generica in modo tale da poter adattare o estendere gli XSD prodotti senza richiedere modifiche significative di tali specifiche.

Le specifiche si applicano ai modelli previsti dalla legge per gli schemi allegati al regolamento (UE) 2018/1727, ai messaggi predefiniti o ai messaggi a testo libero utilizzati negli scambi a norma di tale regolamento.

2.1. *Considerazioni generali*

Le disposizioni esposte qui di seguito si applicano a tutti gli schemi previsti.

2.1.1. Versioni

Deve essere incluso un attributo versione che faciliti la gestione delle versioni degli schemi e consenta di aggiornarli nelle future iterazioni in linea con i requisiti operativi. L'attributo versione deve indicare se la nuova versione è retrocompatibile al momento dell'introduzione di nuove caratteristiche o miglioramenti.

2.1.2. Dichiarazione degli schemi e metadati

— Se del caso, lo schema si avvale di standard o vocabolari pertinenti, richiesti da e-CODEX per consentire l'interoperabilità e necessari per la corretta convalida degli elementi e dei tipi definiti in tale schema. Ciò può comprendere:

  — il vocabolario di base dell'UE della giustizia elettronica;

  — tipi di dati non qualificati;

  — un elenco di codici per i codici linguistici dell'Unione europea.

— Inoltre, se del caso, gli schemi possono incorporare le pertinenti norme ETSI per utilizzare le loro definizioni.

2.1.3. Annotazioni e documentazione

— **Annotazioni**: Di norma ciascun elemento dello schema è accompagnato da annotazioni. Le annotazioni forniscono informazioni leggibili dall'uomo sull'elemento, e spesso ne definiscono la finalità o l'utilizzo in modo chiaro e conciso.

2.1.4. Utilizzo e adattabilità

Lo schema segue le norme di cui alle lettere da a) a d):

a) **Struttura modulare**: ogni sezione è progettata con funzionalità specifiche e può essere riutilizzata o adattata in modo indipendente. Ciò rende facile personalizzare lo schema per i diversi casi d'uso.

b) **Estensibilità**: lo schema è progettato per consentire l'inclusione di nuovi elementi o attributi qualora in futuro siano necessarie informazioni supplementari. Ciò è ottenuto utilizzando elementi e sequenze facoltativi che possono essere estesi senza interrompere il funzionamento delle applicazioni esistenti.

c) **Struttura adattabile**: lo schema è progettato in modo da consentire l'aggiunta o la modifica di elementi o tipi di dati, a seconda delle necessità. La struttura dello schema integra eventuali modifiche dei requisiti senza che sia necessaria una riprogettazione approfondita.

d) **Elementi facoltativi**: gli elementi di uno schema possono essere contrassegnati come facoltativi, ossia possono essere inclusi o omessi in funzione di circostanze specifiche.

Lo schema è progettato per consentire la raccolta di dati strutturati per richieste specifiche.

2.1.5. Modifiche

La progettazione dello schema è caratterizzata da flessibilità, modularità e facilità di adattamento. I tipi complessi e gli elementi facoltativi sono presi in considerazione nella progettazione in modo tale da poter gestire scenari diversi conservando la facilità di intervento in caso di modifica o estensione.

2.2. *Scambio di dati strutturati*

I dati strutturati di cui ai punti 2.2.1 e 2.2.2 sono forniti conformemente all'articolo 22 *bis*, paragrafo 3, del regolamento (UE) 2018/1727. Lo schema permette inoltre di indicare le serie di dati da cancellare nei futuri aggiornamenti.

2.2.1. Dati del registro giudiziario europeo antiterrorismo

Le seguenti specifiche tecniche per lo schema di dati stabiliscono un quadro strutturato per la creazione dello schema in formato XML.

a) Sezione di primo livello

questa sezione di primo livello corrisponde alle informazioni di cui all'allegato III del regolamento (UE) 2018/1727, relativo alle informazioni per il registro giudiziario europeo antiterrorismo (CTR).

b) Struttura del messaggio

la struttura dei dati CTR è costituita da una sequenza di elementi e comprende almeno i seguenti:

i) informazioni per l'identificazione delle persone fisiche:

— cognome;

— nome o nomi;

— pseudonimi;

— data di nascita;

— luogo di nascita (città e paese);

— cittadinanza o le cittadinanze;

— documento di identificazione (tipo e numero del documento);

— genere;

— luogo di residenza;

ii) informazioni per l'identificazione delle persone giuridiche:

— ragione sociale;

— forma giuridica;

— luogo della sede centrale;

iii) informazioni per l'identificazione delle persone sia fisiche sia giuridiche:

— numeri di telefono;

— indirizzi e-mail;

— dettagli dei conti detenuti presso banche o altri istituti finanziari;

— stato del procedimento;

iv) informazioni sul reato:

— informazioni sulle persone giuridiche coinvolte nella preparazione o nella commissione di un reato di terrorismo;

— qualificazione giuridica del reato ai sensi del diritto nazionale;

— forma grave di criminalità applicabile dall'elenco di cui all'allegato I;

— appartenenza a un gruppo terroristico;

— tipo di terrorismo, ad esempio jihadista, separatista, di sinistra o di destra;

— breve sintesi del caso;

v) informazioni sul procedimento nazionale:

— stato di tale procedimento;

— procura competente;

— numero del fascicolo;

— data di avvio del procedimento giudiziario formale;

— collegamenti con altri casi pertinenti;

vi) campo per informazioni aggiuntive (testo libero)

vii) codice dell'autorizzazione preliminare.

2.2.2. Dati trasmessi a norma dell'articolo 21 del regolamento (UE) 2018/1727

a) Articolo 21, paragrafo 4, del regolamento (UE) 2018/1727, relativo all'istituzione di squadre investigative comuni («SIC»)

i) Sezione di primo livello
Questa sezione di primo livello corrisponde alle informazioni di cui all'articolo 21, paragrafo 4, del regolamento (UE) 2018/1727 relative all'istituzione delle SIC.

ii) Struttura del messaggio
La struttura dei dati è costituita da una sequenza di elementi e comprende almeno i seguenti:

— Autorità giudiziaria nazionale incaricata del procedimento penale

— Numero di riferimento nazionale del procedimento penale

— Stato del procedimento penale

— Reati oggetto di indagini

— Altri paesi coinvolti nel caso

— Caso già supportato da Eurojust?

— In caso affermativo, ID del caso Eurojust?

— In caso negativo, si tratta di una richiesta di sostegno?

— Caso supportato da Europol?

— In caso affermativo, task force operativa e/o applicazione di rete per lo scambio sicuro di informazioni («SIENA»)?

— Accordo SIC:

— Paesi interessati

— Parti della SIC (autorità nazionali incaricate delle indagini)

— Numero di riferimento nazionale del procedimento penale oggetto della SIC

— Data della firma

— Durata

— Reati oggetto di indagini

— Breve sintesi del caso

— Principali indagati nel procedimento penale oggetto della SIC (nome, cognome, data e luogo di nascita ed eventualmente altre categorie di dati pertinenti e necessarie di cui all'allegato II)

— Risultati del lavoro delle SIC:

— Difficoltà/ritardi:

— nell'istituzione della SIC

— nel richiedere/condividere prove all'interno della SIC

— nel concordare/attuare una strategia comune in materia di azione penale

— Ammissibilità/inammissibilità/valutazione delle prove della SIC nei procedimenti nazionali

— Esito dei procedimenti giudiziari (esito positivo/negativo dell'azione penale e condanne/assoluzioni)

iii) Codice dell'autorizzazione preliminare

b) Articolo 21, paragrafo 5, del regolamento (UE) 2018/1727, gravi casi complessi

i) Sezione di primo livello

Questa sezione di primo livello corrisponde alle informazioni di cui all'articolo 21, paragrafo 5, del regolamento Eurojust, ossia i casi complessi più gravi.

ii) Struttura del messaggio

La struttura dei dati è costituita da una sequenza di elementi e comprende almeno i seguenti:

— Autorità giudiziaria nazionale incaricata del procedimento penale

— Numero di riferimento nazionale del procedimento penale

— Stato del procedimento penale

— Reati oggetto di indagini

— Altri paesi coinvolti nel caso

— Caso già supportato da Eurojust?

— In caso affermativo, ID del caso Eurojust?

— In caso negativo, si tratta di una richiesta di sostegno?

— Caso supportato da Europol?

— In caso affermativo, task force operativa e/o SIENA?

— Forma grave di criminalità applicabile

— Coinvolgimento di una rete di criminalità organizzata

— Di stampo mafioso

— Rete di criminalità organizzata transnazionale

— Ripercussioni a livello europeo

— Principali indagati nel procedimento penale (nome, cognome, data e luogo di nascita ed eventualmente altre categorie di dati pertinenti e necessarie di cui all'allegato II)

— Breve sintesi del caso

— Altri paesi coinvolti

— Paesi con i quali è già stata avviata la cooperazione

— Autorità competenti coinvolte in un altro paese

— Strumenti di cooperazione giudiziaria utilizzati

— Numero di richieste inviate/ricevute

— Esistenza di indagini collegate

— Paesi con i quali attivare la cooperazione/paesi potenzialmente interessati

— Tipo di cooperazione necessaria (ad esempio estradizione, raccolta di prove, altra cooperazione)

— Esistenza di indagini collegate

iii) Codice dell'autorizzazione preliminare

c) Articolo 21, paragrafo 6, lettera a), del regolamento (UE) 2018/1727, conflitti di giurisdizione

i) Sezione di primo livello

Questa sezione di primo livello corrisponde alle informazioni di cui all'articolo 21, paragrafo 6, lettera a), del regolamento (UE) 2018/1727 relativo ai conflitti di giurisdizione.

ii) Struttura del messaggio

La struttura dei dati è costituita da una sequenza di elementi e comprende almeno i seguenti:

— Autorità giudiziaria nazionale incaricata del procedimento penale

— Numero di riferimento nazionale del procedimento penale

— Stato del procedimento penale (ad esempio indagine, azione penale, processo)

— Reati oggetto di indagini

— Altri paesi coinvolti nel caso

— Caso già supportato da Eurojust?

— In caso affermativo, ID del caso Eurojust?

— In caso negativo, si tratta di una richiesta di sostegno?

— Caso supportato da Europol?

— In caso affermativo, task force operativa e/o SIENA?

— Altri paesi coinvolti

— Autorità nazionali competenti dell'altro paese, se note

— Numero di riferimento nazionale del procedimento penale nell'altro paese

— Fase del procedimento nell'altro paese, se noto

— Conflitto positivo o negativo

— Conflitto effettivo o potenziale

— Attività di coordinamento già intraprese (ad esempio consultazioni a norma della decisione quadro 2009/948/JHA del Consiglio ([1]))

— Breve sintesi del caso

— Principali indagati comuni (nome, cognome, data e luogo di nascita ed eventualmente altre categorie di dati pertinenti e necessarie di cui all'allegato II)

iii) Codice dell'autorizzazione preliminare

d) Articolo 21, paragrafo 6, lettera b), consegne controllate

i) Sezione di primo livello
Questa sezione di primo livello corrisponde alle informazioni di cui all'articolo 21, paragrafo 6, lettera b), del regolamento (UE) 2018/1727: consegne controllate

ii) Struttura del messaggio
La struttura dei dati è costituita da una sequenza di elementi e comprende almeno i seguenti:

— Autorità giudiziaria nazionale incaricata del procedimento penale

— Numero di riferimento nazionale del procedimento penale

— Stato del procedimento penale (ad esempio indagine, azione penale, processo)

— Reati oggetto di indagini

— Altri paesi coinvolti nel caso

— Caso già supportato da Eurojust?

— In caso affermativo, ID del caso Eurojust?

— In caso negativo, si tratta di una richiesta di sostegno?

— Caso supportato da Europol?

— In caso affermativo, task force operativa e/o SIENA?

— Altri paesi coinvolti

— Paese di origine/transito/destinazione finale

— Autorità nazionali competenti in altri paesi

— Esistenza di indagini collegate in altri paesi

([1]) Decisione quadro 2009/948/GAI del Consiglio, del 30 novembre 2009, sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali (GU L 328 del 15.12.2009, pag. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Tipo di merci consegnate (ad esempio sostanze stupefacenti e tipo/denaro/armi/sigarette/altro)

— Stato della consegna controllata (ad esempio prevista, in corso, completata)

— Esito della consegna controllata, se già effettuata

— Strumento di cooperazione giudiziaria utilizzato

— Principali indagati comuni (nome, cognome, data e luogo di nascita ed eventualmente altre categorie di dati pertinenti e necessarie di cui all'allegato II)

iii) Codice dell'autorizzazione preliminare

e) Articolo 21, paragrafo 6, lettera c), del regolamento (UE) 2018/1727, difficoltà ripetute con gli strumenti di cooperazione giudiziaria

i) Sezione di primo livello

Questa sezione di primo livello corrisponde alle informazioni di cui all'articolo 21, paragrafo 6, lettera c), del regolamento (UE) 2018/1727: difficoltà ripetute con gli strumenti di cooperazione giudiziaria

ii) Struttura del messaggio

La struttura dei dati è costituita da una sequenza di elementi e comprende almeno i seguenti:

— Autorità giudiziaria nazionale incaricata del procedimento penale

— Numero di riferimento nazionale del procedimento penale

— Stato del procedimento penale (ad esempio indagine, azione penale, processo)

— Reati oggetto di indagini

— Altri paesi coinvolti nel caso

— Caso già supportato da Eurojust?

— In caso affermativo, ID del caso Eurojust?

— In caso negativo, si tratta di una richiesta di sostegno?

— Caso supportato da Europol?

— In caso affermativo, task force operativa e/o SIENA?

— Altri paesi coinvolti

— Autorità nazionali competenti, se note

— Facente funzione di autorità di emissione o di esecuzione

— Strumento di cooperazione giudiziaria in questione (ad esempio MAE, OEI, congelamento e confisca)

— Richiesta specifica in questione (ossia quale atto di indagine, quale tipo di congelamento, MAE per l'esecuzione di una pena o per l'azione penale)

— Rifiuto o difficoltà ripetute

— In caso di rifiuto indicare il motivo specifico invocato

— Breve descrizione della questione

— Altre autorità nazionali interessate dalla stessa questione, se del caso

iii) Codice dell'autorizzazione preliminare

2.3. *Codici dell'autorizzazione preliminare*

Quando condividono dati con Eurojust tramite JUDEX, le autorità nazionali competenti indicano, mediante codici di autorizzazione preliminare, l'ulteriore trattamento, accesso e trasferimento dei dati a seguito dell'identificazione di un collegamento. I codici di autorizzazione preliminare indicano se e in quale misura le informazioni relative al collegamento possono essere condivise con altre autorità nazionali competenti, altre agenzie e organismi dell'Unione, paesi terzi o organizzazioni internazionali.

2.4. *Messaggi predefiniti*

I messaggi predefiniti sono rappresentazioni di scambi istituiti dal regolamento (UE) 2018/1727, ma per i quali non è stata disposta alcuna forma specifica dall'atto giuridico. Le tipologie e il numero di tali scambi sono determinati nell'ambito dell'analisi operativa e tecnica.

Le definizioni XML Schema Definition (XSD) per i messaggi predefiniti sono concepite in modo da garantire la coerenza, la struttura e la conformità alle esigenze operative.

A tali schemi si applica quanto segue:

a) il nome della sezione di primo livello di questo schema dipende dal tipo specifico di messaggio definito;

b) i campi necessari per lo specifico tipo di messaggio sono aggiunti e definiti all'interno della struttura, garantendo un'adeguata rappresentazione dei dati.

2.5. *Messaggi a testo libero*

I messaggi a testo libero sono rappresentazioni di scambi che accettano contenuti non strutturati o parzialmente strutturati, offrendo flessibilità nel rispetto dei requisiti normativi e commerciali. Gli XSD per i messaggi a testo libero sono progettati in modo da garantire la coerenza e la corretta formattazione.

A tali schemi si applica quanto segue:

a) il nome della sezione di primo livello nello schema dipende dal tipo specifico di messaggio a testo libero definito;

b) lo schema definisce la struttura necessaria per il messaggio a testo libero, e offre nel contempo un ordinamento adeguato degli elementi richiesti;

c) i campi necessari per lo specifico tipo di messaggio a testo libero sono aggiunti e definiti all'interno della struttura, garantendo un'adeguata rappresentazione dei dati.

ALLEGATO III

SPECIFICHE TECNICHE DELLE IMPRONTE DIGITALI E DELLE FOTOGRAFIE

I messaggi scambiati attraverso il sistema informatico decentrato possono essere accompagnati da allegati, tra cui file dell'Istituto nazionale per gli standard e la tecnologia («NIST») contenenti impronte digitali e fotografie, conformemente alle specifiche tecniche di cui ai punti 1 e 2.

1. **Impronte digitali**

Le impronte digitali che possono essere condivise con Eurojust ai fini dell'identificazione affidabile delle persone oggetto di procedimenti penali connessi a reati di terrorismo soddisfano le condizioni seguenti:

a) le impronte digitali sono fornite in un unico file contenente le immagini dattiloscopiche digitali (file NIST relativo alle impronte digitali) e sono trasmesse conformemente alla norma ANSI/NIST-ITL 1-2011 aggiornata al 2015 (o versione più recente);

b) i file NIST relativo alle impronte digitali comprendono fino a dieci impronte digitali individuali: piatte, rollate o entrambe;

c) tutte le impronte digitali sono etichettate;

d) le impronte digitali sono acquisite mediante scansione diretta (live-scan) o sono inchiostrate su carta, a condizione che quelle rilevate con quest'ultima modalità siano scansionate con la risoluzione richiesta e con la stessa qualità;

e) il file NIST relativo alle impronte digitali consente l'inserimento di informazioni complementari quali le condizioni di registrazione delle impronte digitali e il metodo utilizzato per l'acquisizione delle immagini delle impronte digitali individuali;

f) i dati relativi alle impronte digitali hanno una risoluzione nominale di 500 o 1 000 ppi [1] (e uno scarto tollerato di +/- 10 ppi) e 256 livelli di grigio;

g) l'algoritmo di compressione delle impronte digitali da utilizzare segue le raccomandazioni dell'Istituto nazionale per gli standard e la tecnologia. I dati relativi alle impronte digitali con una risoluzione di 500 ppi sono compressi utilizzando l'algoritmo WSQ (ISO/IEC 19794-5:2005). I dati relativi alle impronte digitali con una risoluzione di 1 000 ppi sono compressi utilizzando lo standard di compressione delle immagini JPEG 2000 (ISO/IEC 15444-1) e il sistema di codifica. Il grado di compressione da ottenere è 15:1.

2. **Fotografie**

Le fotografie che possono essere condivise con Eurojust ai fini dell'identificazione affidabile delle persone oggetto di procedimenti penali connessi a reati di terrorismo soddisfano le condizioni seguenti:

a) è fornita una sola immagine del volto in un file fotografico (file fotografico NIST) ed è presentata conformemente alla norma ANSI/NIST-ITL 1-2011, aggiornata al 2015, o versione più recente;

b) le fotografie sono in scala di grigi, a colori o a infrarossi vicini;

c) la qualità delle fotografie è basata sui requisiti per le immagini di tipo frontale di cui alla norma ISO/IEC 19794-5:2011 o qualsiasi versione più recente disponibile;

d) il file fotografico NIST consente l'inserimento di informazioni complementari, compresa la data in cui è stata acquisita l'immagine;

[1] Pixel/pollice.

e) le fotografie, in modalità ritratto, hanno una risoluzione minima di 600 x 800 pixel e una risoluzione massima di 1 200 x 1 600 pixel;

f) il volto occupa uno spazio all'interno della fotografia che garantisce un minimo di 120 pixel tra i centri dei due occhi;

g) l'algoritmo di compressione delle fotografie impiegato segue le raccomandazioni dell'Istituto nazionale per gli standard e la tecnologia. Le fotografie sono compresse una sola volta utilizzando lo standard di compressione delle immagini JPG (ISO/IEC 10918) o JPEG 2000 (ISO/IEC 15444) e il sistema di codifica, con un grado di compressione delle immagini massimo consentito pari a 20:1.