2025/1550

29.7.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/1550 DELLA COMMISSIONE

del 28 luglio 2025

che stabilisce le specifiche tecniche e gli altri requisiti tecnici per il sistema informatico decentrato di cui al regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il 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 ([1]), in particolare l'articolo 25, paragrafo 1, lettere a), b), c) e d),

considerando quanto segue:

(1) Allo scopo di istituire il sistema informatico decentrato di cui al regolamento (UE) 2023/1543, è necessario definire e adottare specifiche tecniche, misure tecniche e obiettivi tecnici per l'attuazione di tale sistema.

(2) Conformemente al regolamento (UE) 2023/1543, il sistema informatico decentrato dovrebbe comprendere i sistemi informatici degli Stati membri e delle agenzie e degli organi dell'Unione, così come i punti di accesso e-CODEX interoperabili attraverso i quali tali sistemi sono interconnessi. Di conseguenza, le specifiche tecniche e gli altri requisiti tecnici del sistema informatico decentrato dovrebbero rispecchiare tale quadro.

(3) Conformemente al regolamento (UE) 2023/1543, 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]).

(4) 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, sia i sistemi informatici nazionali sia il software di implementazione di riferimento dovrebbero essere soggetti alle stesse specifiche tecniche e agli stessi requisiti tecnici stabiliti nel presente regolamento.

(5) Onde attenuare potenziali problemi tecnici relativi alla capacità e all'affidabilità del sistema informatico decentrato, è necessario stabilire una soglia per il volume di prove elettroniche trasmesse attraverso tale sistema. Dopo l'avvio del sistema la frequenza e il volume di tali trasmissioni dovrebbero essere monitorati e la soglia dovrebbe essere adeguata, se del caso, per massimizzare l'efficienza del sistema.

(6) Al fine di rafforzare l'interoperabilità e l'efficienza del sistema informatico decentrato, dovrebbe essere imposto l'uso di norme ETSI adeguate. È opportuno monitorare gli sviluppi futuri e, se necessario, prendere in considerazione l'adozione di ulteriori norme ETSI.

(7) L'Irlanda è vincolata dal regolamento (UE) 2023/1543 e pertanto partecipa all'adozione del presente regolamento.

(8) 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 è vincolata né è soggetta all'applicazione del presente regolamento.

([1]) GU L 191 del 28.7.2023, pag. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/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).

(9) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([3]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 25 giugno 2025.

(10) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 26 del regolamento (UE) 2023/1543,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Specifiche tecniche del sistema informatico decentrato

Le specifiche tecniche, i requisiti tecnici, le misure tecniche e gli obiettivi tecnici del sistema informatico decentrato di cui all'articolo 25, paragrafo 1, del regolamento (UE) 2023/1543 per la comunicazione ai sensi dell'articolo 19 di tale regolamento sono stabiliti nell'allegato del presente regolamento.

Articolo 2

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 28 luglio 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

([3]) 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

SPECIFICHE TECNICHE DEL SISTEMA INFORMATICO DECENTRATO

(di cui all'articolo 1)

1. Introduzione e oggetto

Il presente allegato stabilisce le specifiche tecniche, le misure tecniche e gli obiettivi tecnici del sistema informatico decentrato per le procedure di cui al regolamento (UE) 2023/1543.

A norma del regolamento (UE) 2023/1543, in particolare dell'articolo 19, il sistema informatico decentrato deve consentire la comunicazione scritta tra le autorità competenti e gli stabilimenti designati o i rappresentanti legali, tra le autorità competenti, come pure tra le autorità competenti e le agenzie o gli organismi competenti dell'Unione.

2. Definizioni

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. «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, moduli, documenti e prove elettroniche attraverso il sistema informatico decentrato;

2.8. «API»: interfaccia di programmazione di applicazioni basata su una norma comune per lo scambio dei dati, che consente ai prestatori di servizi che si avvalgono di soluzioni informatiche su misura ai fini dello scambio di informazioni e dati relativi alle richieste di prove elettroniche di accedere ai sistemi informatici decentrati con mezzi automatizzati;

2.9. «interfaccia web»: interfaccia utente disponibile tramite HTTPS su Internet, che consente ai prestatori di servizi di accedere al sistema informatico decentrato con mezzi manuali per comunicare in modo sicuro con le autorità e scambiare informazioni e dati relativi alle richieste di prove elettroniche, senza dover creare una propria infrastruttura dedicata;

2.10. «norme ETSI»: norme e specifiche tecniche elaborate dall'Istituto europeo per le norme di telecomunicazione (ETSI) per garantire l'interoperabilità, la sicurezza e l'efficienza delle tecnologie dell'informazione e della comunicazione. Forniscono quadri, protocolli e migliori pratiche per un'ampia gamma di tecnologie, tra cui reti mobili, comunicazioni radio, cibersicurezza e infrastrutture Internet;

2.11. «valore di hash»: output a lunghezza fissa generato da una funzione di hash crittografico applicata a un input di lunghezza arbitraria. Una funzione di hash crittografico è concepita per soddisfare le proprietà fondamentali di sicurezza, tra cui la resistenza alla preimmagine, la resistenza alla seconda preimmagine e la resistenza alla collisione, garantendone la robustezza contro attacchi di collisione e inversione;

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

2.13. «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;

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

2.15. «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;

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

2.17. «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 della comunicazione scritta tra le autorità competenti degli Stati membri, tra le autorità competenti e gli stabilimenti designati o i rappresentanti legali dei prestatori di servizi, come pure tra le autorità competenti e le agenzie o gli organismi dell'Unione, il sistema informatico decentrato utilizza metodi di comunicazione basati sui servizi, come servizi web o altri componenti e soluzioni software riutilizzabili per lo scambio dei dati. Nello specifico, comporterà 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 supporterà la comunicazione attraverso il sistema e-CODEX.

3.2. Dato l'elevato volume previsto di prove elettroniche da trasmettere a seguito di un ordine europeo di produzione attraverso il sistema informatico decentrato, come indicato all'articolo 19, paragrafi 1 e 4, del regolamento (UE) 2023/1543, che potrebbe comportare vincoli di capacità tecnica che potrebbero incidere negativamente sul sistema informatico decentrato, le prove elettroniche sono trasmesse attraverso tale sistema nella misura in cui non superano la soglia di 25 megabyte (25 600 kilobyte). La trasmissione di prove elettroniche superiori a tale soglia è effettuata conformemente all'articolo 19, paragrafo 5, di detto regolamento.

3.3. Visto l'articolo 19, paragrafo 6, del regolamento (UE) 2023/1543, nel caso in cui la trasmissione avvenga con mezzi alternativi come previsto in tale paragrafo a causa dell'impossibilità di utilizzo del sistema informatico decentrato per uno dei motivi di cui all'articolo 19, paragrafo 5, di tale regolamento:

3.3.1. Se la trasmissione riguarda una comunicazione scritta, compreso lo scambio di moduli, tra le autorità competenti e i prestatori di servizi ai sensi dell'articolo 19, paragrafo 1, del regolamento (UE) 2023/1543, l'originatore della trasmissione registra la trasmissione nel proprio sistema informatico nazionale facente parte del sistema informatico decentrato. Le informazioni registrate comprendono almeno il numero di riferimento del caso o del fascicolo, la data e l'ora, il mittente e il destinatario, il nome del fascicolo e le sue dimensioni.

3.3.2. Se la trasmissione riguarda una comunicazione scritta, compreso lo scambio di moduli, tra le autorità competenti, o una comunicazione scritta con le agenzie o gli organismi competenti dell'Unione ai sensi dell'articolo 19, paragrafo 4, del regolamento (UE) 2023/1543, l'originatore della trasmissione registra la trasmissione nel sistema informatico decentrato, nello specifico all'interno del suo sistema informatico nazionale o, se del caso, nei sistemi informatici gestiti dall'agenzia o dall'organismo competente dell'Unione. Le informazioni registrate comprendono almeno il numero di riferimento del caso o del fascicolo, la data e l'ora della trasmissione, il mittente e il destinatario, il nome del fascicolo e le sue dimensioni.

3.3.3. Nel caso in cui le prove elettroniche a seguito di un ordine europeo di produzione siano state trasmesse mediante mezzi di comunicazione alternativi tra i prestatori di servizi e le autorità competenti dello Stato di emissione ([1]), o nel caso in cui le prove elettroniche siano trasmesse con mezzi alternativi dall'autorità di esecuzione alle autorità competenti dello Stato di emissione secondo la procedura di esecuzione di cui all'articolo 16, paragrafo 9, del regolamento (UE) 2023/1543, l'originatore:

a) registra e trasmette all'autorità cui sono state trasmesse o messe a disposizione le prove elettroniche, nell'ambito di un avviso, le seguenti informazioni:

1) informazioni sul mittente e sul destinatario;

2) metadati che associano le prove elettroniche fornite a uno o più ordini europei di produzione o di conservazione;

3) la data e l'ora della trasmissione o l'indicazione del momento in cui le prove elettroniche sono state messe a disposizione del destinatario;

4) informazioni relative ai mezzi di trasmissione (ad esempio una registrazione del link sicuro attraverso il quale le prove elettroniche sono state messe a disposizione, una prova della ricezione o della consegna da parte dei servizi postali ecc. ([2]));

5) i nomi completi dei fascicoli delle prove elettroniche trasmesse o altrimenti messe a disposizione del destinatario previsto nello Stato di emissione;

6) le dimensioni dei dati delle prove elettroniche trasmesse o altrimenti messe a disposizione del destinatario previsto nello Stato di emissione;

7) almeno un valore di hash dei dati trasmessi o messi a disposizione e un'indicazione dell'algoritmo o degli algoritmi di hash utilizzati. L'algoritmo o gli algoritmi di hash utilizzati per il calcolo del valore/dei valori di hash devono essere robusti dal punto di visto crittografico, di uso comune, e non soggetti a debolezze pubblicamente divulgate come le collisioni (ad esempio SHA-512, SHA3-512, BLAKE2 o RIPEMD-160, ma potenzialmente più robusti, a seconda degli sviluppi tecnologici);

b) se del caso, indica, nell'ambito dell'avviso di cui alla lettera a), la data e l'ora fino alle quali le prove elettroniche rimarranno accessibili. Tale termine fornisce all'autorità competente dello Stato di emissione un arco di tempo ragionevole per il recupero delle prove elettroniche, che non può essere inferiore a 10 giorni di calendario e non superiore a 45 giorni di calendario dal momento in cui le prove elettroniche sono messe a disposizione. Su richiesta dell'autorità competente dello Stato di emissione, il termine indicato dall'originatore può essere prorogato in casi individuali;

c) può registrare e trasmettere eventuali informazioni o osservazioni supplementari rilevanti per il caso all'autorità alla quale le prove elettroniche sono state trasmesse o rese disponibili, nell'ambito dell'avviso di cui alla lettera a).

3.4. Visto l'articolo 28 del regolamento (UE) 2023/1543, il software di implementazione di riferimento programmaticamente raccoglie, trasmette o fornisce in altro modo l'accesso alle statistiche di cui al paragrafo 2 di tale articolo in formati di dati strutturati (ad esempio XML) e non strutturati (ad esempio PDF). Conformemente all'articolo 28, paragrafo 3, del regolamento (UE) 2023/1543, se tecnicamente attrezzati, anche i portali nazionali ([3]) gestiti dagli Stati membri possono trasmettere o fornire tali statistiche alla Commissione mediante un processo automatizzato. La Commissione pubblica orientamenti sulla struttura dei dati e sul metodo di raccolta e comunicazione di tali statistiche.

([1]) Per maggiore chiarezza, i riferimenti alle autorità nazionali competenti si intendono fatti, *mutatis mutandis*, anche ai membri nazionali di Eurojust, ai procuratori europei e ai procuratori europei delegati, nella misura in cui sono autorizzati a svolgere le stesse funzioni ai sensi del diritto dell'UE e del diritto nazionale.

([2]) È opportuno ricordare che, a norma dell'articolo 19, paragrafo 5, la trasmissione attraverso tali mezzi di comunicazione alternativi deve soddisfare i requisiti di rapidità, sicurezza e affidabilità, consentendo al ricevente di stabilire l'autenticità.

([3]) Con «portali nazionali» si dovrebbero intendere i «sistemi informatici» nazionali che fanno parte del sistema informatico decentrato quale definito all'articolo 3, punto 21), del regolamento (UE) 2023/1543.

4. **Protocolli di comunicazione**

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

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

b) la comunicazione tra le autorità competenti e le agenzie e gli organismi dell'Unione all'interno del sistema informatico decentrato;

c) la comunicazione tra le autorità competenti e i prestatori di servizi attraverso un'API e l'interfaccia web, e

d) la comunicazione con la banca dati degli organi giurisdizionali.

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, in particolare su quelli cui fanno riferimento gli organismi europei di normazione, come ETSI.

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 per le prove elettroniche si avvalgono di standard o vocabolari pertinenti, necessari per la corretta convalida degli elementi e dei tipi definiti in tale schema. Questi possono includere:

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.

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

4.6. La Commissione definisce le specifiche per l'API comune, che gli Stati di esecuzione mettono a disposizione dei prestatori di servizi come mezzo di accesso al sistema informatico decentrato. Per quanto possibile e ragionevole, tale API si basa sulla specifica tecnica ETSI TS 104 144 («*Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers*» - «Definizione dell'interfaccia ai fini del regolamento sulle prove elettroniche (UE) 2023/1543 per le autorità nazionali e i prestatori di servizi»).

4.7. 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 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 (messaggi, moduli, documenti e prove elettroniche) 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 la disponibilità garantendo un accesso continuo ai servizi e ai dati e prevenendo interruzioni dovute ad attacchi informatici o guasti;

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

f) 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. 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.

5.4. 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 ([4]) e della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([5]), a seconda dei casi.

5.5. Gli Stati membri che utilizzano un sistema informatico 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.

5.6. Vista la loro partecipazione al sistema informatico decentrato, Eurojust e la Procura europea attuano le misure necessarie per garantire che i loro rispettivi sistemi informatici siano conformi ai requisiti del regolamento (UE) 2018/1725 e dei loro atti costitutivi.

5.7. Gli Stati membri, Eurojust e la Procura europea 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 loro rispettive politiche rilevanti, per i sistemi informatici soggetti alla loro competenza che fanno parte del sistema informatico decentrato.

6. **Cifratura** ([6]) **delle prove elettroniche**

6.1. Ferme restando le misure di sicurezza previste dal sistema informatico decentrato le autorità competenti, nell'emettere un ordine europeo di produzione, possono fornire, in più, un apposito certificato pubblico X.509 per la cifratura asimmetrica delle prove elettroniche.

([4]) 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).

([5]) 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).

([6]) Per evitare dubbi, il termine «prove elettroniche» è limitato alla definizione di cui all'articolo 3, punto 8), del regolamento (UE) 2023/1543.

6.2. Il rilascio, la gestione, la verifica e tutti gli aspetti correlati dei certificati di cui al punto 6.1, unitamente alla corrispondente infrastruttura a chiave pubblica, sono di esclusiva responsabilità dello Stato di emissione.

6.3. Fatti salvi i futuri sviluppi tecnologici, i certificati pubblici supportano algoritmi di cifratura standard del settore, quali RSA (*Rivest-Shamir-Adleman*) o ECDH (*Ellitical Curve Diffie-Hellman* - curve ellittiche Diffie-Hellman) per ECC (*Elliptic Curve Cryptography* - cifratura a curve ellittiche).

6.4. I certificati pubblici recano l'estensione «keyUsage» appropriata, come «keyEncipherment» o «dataEncipherment» per i certificati basati sull'RSA, e «keyAgreement» per i certificati basati sull'ECC. I certificati sono messi a disposizione in formato PEM (*Privacy-Enhanced Mail* - e-mail a privacy aumentata) o DER (*Distinguished Encoding Rules* - regole di codifica distinte).

6.5. Qualora l'autorità di emissione abbia fornito un certificato pubblico X.509 e qualora un prestatore di servizi invii le prove elettroniche prodotte a seguito di un ordine europeo di produzione, il prestatore, prima della trasmissione di tali dati attraverso il sistema informatico decentrato, cripta le prove elettroniche utilizzando il rispettivo certificato pubblico X.509 fornito dallo Stato di emissione.

6.6. Qualora l'autorità di emissione abbia fornito un certificato pubblico X.509, ma la trasmissione delle prove elettroniche in forma cifrata non sia possibile per motivi tecnici o altri motivi giustificabili, e fatta salva la disposizione di cui all'articolo 19, paragrafo 5, del regolamento (UE) 2023/1543, il fornitore di servizi può trasmettere i dati senza cifratura del contenuto. In tali casi il prestatore di servizi fornisce una spiegazione motivata all'autorità di emissione.

7. **Obiettivi minimi di disponibilità**

7.1. Gli Stati membri, Eurojust e la Procura europea 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.

7.2. 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.

7.3. 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.

7.4. Gli Stati membri, Eurojust e la Procura europea notificano alla Commissione 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.

7.5. Qualora gli Stati membri, Eurojust o la Procura europea abbiano stabilito periodi di manutenzione regolari, comunicano alla Commissione e ai partecipanti al sistema informatico decentrato l'ora e il giorno/i giorni in cui sono programmati tali periodi fissi regolari. Fatti salvi gli obblighi di cui al punto 7.4, in caso di indisponibilità, durante tale periodo fisso regolare, di componenti del sistema informatico decentrato soggetti alla loro competenza, gli Stati membri, Eurojust o la Procura europea non sono tenuti a comunicare ogni volta alla Commissione tale indisponibilità.

7.6. In caso di guasto tecnico imprevisto dei componenti del sistema informatico decentrato soggetti alla loro competenza, gli Stati membri, Eurojust o la Procura europea ne informano immediatamente la Commissione e i partecipanti al sistema informatico decentrato e, se noto, indicano il previsto periodo di ripristino.

7.7. In caso di attività di manutenzione o di guasto tecnico imprevisto di componenti del sistema informatico decentrato soggetti alla competenza di uno Stato membro, con ripercussioni negative sulla disponibilità dell'API e/o dell'interfaccia web per i prestatori di servizi, lo Stato membro interessato rende tempestivamente note tali informazioni su un sito web e/o le comunica ai prestatori di servizi che operano nel suo territorio senza indebito ritardo.

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

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

7.10. Gli Stati membri, Eurojust e la Procura europea attuano misure adeguate per conseguire gli obiettivi di disponibilità sopra indicati e stabiliscono procedure per rispondere efficacemente agli incidenti.

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

8.1. Visto l'articolo 19 del regolamento (UE) 2023/1543, ai fini del funzionamento del sistema informatico decentrato è fondamentale istituire una banca dati accreditata dei prestatori di servizi e delle autorità competenti.

8.2. Tale banca dati accreditata delle autorità competenti contiene le seguenti informazioni in un formato strutturato:

a) ai fini dell'articolo 19 del regolamento (UE) 2023/1543, informazioni sulle autorità competenti notificate a norma dell'articolo 31, paragrafo 1, lettere da a) a c), del medesimo regolamento, riguardanti anche:

1) i membri nazionali di Eurojust, con l'indicazione se essi sono autorizzati a norma del diritto nazionale a emettere ordini europei di produzione e ordini europei di conservazione conformemente all'articolo 8, paragrafi 3 e 4, del regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio ([7]);

2) i procuratori europei delegati e i procuratori europei, se notificati dagli Stati membri a norma dell'articolo 105, paragrafo 3, del regolamento (UE) 2017/1939 del Consiglio ([8]) quale autorità d'emissione competente ai sensi del regolamento (UE) 2023/1543;

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

c) informazioni necessarie per il corretto funzionamento degli scambi di dati e l'instradamento tecnico dei messaggi nel contesto di tali scambi all'interno del sistema informatico decentrato.

8.2.1. Le informazioni di cui al punto 8.2., lettera c), includono:

a) informazioni sullo Stato membro in cui il prestatore di servizi ha lo stabilimento designato o in cui risiede il suo rappresentante legale:

1) Stato membro;

2) autorità centrale;

([7]) Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, del 14 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 (GU L 295 del 21.11.2018, pag. 138).

([8]) Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO») (GU L 283 del 31.10.2017, pag. 1).

b) informazioni sul prestatore di servizi:

1) nome;

2) indirizzo/sede;

3) numero di registrazione;

4) forma giuridica;

5) numero di telefono;

6) indirizzo e-mail;

c) informazioni sullo stabilimento designato/sul rappresentante legale:

1) tipo di soggetto (stabilimento designato/rappresentante legale);

2) nome;

3) indirizzo/sede;

4) numero di telefono;

5) indirizzo e-mail;

6) persona/soggetto di contatto generale;

7) lingua/lingue ufficiali accettate dal prestatore di servizi/dallo stabilimento designato/dal rappresentante legale;

8) servizi di cui all'articolo 2, paragrafo 1, della direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio ([9]) offerti nell'Unione;

9) tipo di strumenti giuridici dell'UE per i quali è designato lo stabilimento designato/il rappresentante legale (nelle situazioni in cui gli Stati membri non partecipano a tutti gli strumenti giuridici dell'UE rilevanti);

10) ambito territoriale della designazione/della nomina;

d) autenticazione delle informazioni:

1) nome del rappresentante autorizzato;

2) titolo professionale;

3) indirizzo;

4) numero di telefono;

5) indirizzo e-mail;

6) data.

8.2.2. Le informazioni di cui al punto 8.2, lettera c), possono includere, ove disponibili:

a) informazioni sul prestatore di servizi:

1) referente per le domande sulle notifiche (se diverso dal firmatario);

2) sito web;

b) tipi di dati disponibili:

1) per ciascun servizio interessato:

— tipi di dati disponibili;

— categoria di dati;

— identificativi;

— periodo di disponibilità dei dati;

([9]) Direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali (GU L 191 del 28.7.2023, pag. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) informazioni supplementari sui dati;

3) informazioni supplementari sul servizio (ad esempio rapporti di subappalto);

c) informazioni sullo stabilimento designato/sul rappresentante legale:

1) altri prestatori di servizi per i quali è designato lo stabilimento designato o il rappresentante legale;

2) informazioni di contatto per l'assistenza tecnica;

3) contatto di emergenza;

d) informazioni tecniche:

1) nome del punto di contatto tecnico;

2) numero di telefono del punto di contatto tecnico;

3) indirizzo e-mail del punto di contatto tecnico;

4) API URL per il recupero dinamico di informazioni sui tipi di dati;

5) tipo di connessione con il sistema informatico nazionale:

— interfaccia web;

— API;

— push API URL.

8.3. In considerazione delle esigenze operative del sistema informatico decentrato:

a) la Commissione è responsabile dello sviluppo, della manutenzione, del funzionamento e del supporto della banca dati accreditata;

b) la Commissione rende possibile l'accesso alla banca dati accreditata tramite un'API messa a disposizione delle autorità competenti, di Eurojust e della Procura europea ai fini della loro partecipazione al sistema informatico decentrato;

c) gli Stati membri provvedono affinché le informazioni sulle loro autorità competenti di cui al punto 8.2, lettere a) e b), contenute nella banca dati accreditata, siano complete, esatte e tenute aggiornate;

d) la banca dati accreditata consente agli Stati membri di fornire e aggiornare le informazioni sui loro prestatori di servizi ivi contenuti, e alle autorità che partecipano al sistema informatico decentrato di accedere programmaticamente a tali informazioni e di recuperarle;

e) gli Stati membri e i prestatori di servizi provvedono affinché le informazioni di cui al punto 8.2, lettera c), contenute nella banca dati accreditata, siano complete, esatte e tenute aggiornate.