REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/1550 AL COMISIEI

din 28 iulie 2025

de stabilire a specificațiilor tehnice și a altor cerințe pentru sistemul informatic descentralizat, menționate în Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale ([1]), în special articolul 25 alineatul (1) literele (a), (b), (c) și (d),

întrucât:

(1) Pentru a institui sistemul informatic descentralizat menționat în Regulamentul (UE) 2023/1543, este necesar să se definească și să se adopte specificații tehnice, măsuri și obiective pentru punerea în aplicare a sistemului respectiv.

(2) În conformitate cu Regulamentul (UE) 2023/1543, sistemul informatic descentralizat ar trebui să fie alcătuit din sistemele informatice ale statelor membre și ale agențiilor și organelor Uniunii și din puncte de acces e-CODEX interoperabile prin care să fie interconectate sistemele informatice respective. În consecință, specificațiile tehnice și alte cerințe ale sistemului informatic descentralizat ar trebui să reflecte acest cadru.

(3) În conformitate cu Regulamentul (UE) 2023/1543, punctele de acces ale sistemului informatic descentralizat ar trebui să se bazeze pe punctele de acces e-CODEX autorizate, astfel cum sunt definite la articolul 3 alineatul (3) din Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului ([2]).

(4) Statele membre pot alege să utilizeze software-ul de implementare de referință dezvoltat de Comisie ca sistem back-end în locul unui sistem informatic național. Pentru a asigura interoperabilitatea, atât sistemele informatice naționale, cât și software-ul de implementare de referință ar trebui să facă obiectul acelorași specificații și cerințe tehnice prevăzute în prezentul regulament.

(5) Pentru a atenua eventualele probleme tehnice legate de capacitatea și fiabilitatea sistemului informatic descentralizat, este necesar să se stabilească un prag pentru volumul de probe electronice transmise prin intermediul sistemului respectiv. În urma lansării sistemului, frecvența și volumul acestor transmisii ar trebui monitorizate, iar pragul ar trebui ajustat, după caz, pentru a maximiza eficiența sistemului.

(6) Pentru a consolida interoperabilitatea și eficiența sistemului informatic descentralizat, ar trebui să se impună utilizarea unor standarde ETSI corespunzătoare. Evoluțiile viitoare ar trebui monitorizate și, dacă este necesar, ar trebui luată în considerare adoptarea unor standarde ETSI suplimentare.

(7) Regulamentul (UE) 2023/1543 este obligatoriu pentru Irlanda și, prin urmare, Irlanda participă la adoptarea prezentului regulament.

(8) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, prezentul regulament nu este obligatoriu pentru Danemarca și nu i se aplică.

([1]) JO L 191, 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului din 30 mai 2022 privind un sistem informatizat pentru schimbul electronic transfrontalier de date în domeniul cooperării judiciare în materie civilă și penală (sistemul e-CODEX) și de modificare a Regulamentului (UE) 2018/1726 (JO L 150, 1.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([3]) și a emis un aviz la 25 iunie 2025.

(10) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit în temeiul articolului 26 din Regulamentul (UE) 2023/1543,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Specificații tehnice ale sistemului informatic descentralizat

Specificațiile și cerințele tehnice, măsurile și obiectivele sistemului informatic descentralizat menționat la articolul 25 alineatul (1) din Regulamentul (UE) 2023/1543 în vederea comunicării în sensul articolului 19 din regulamentul respectiv sunt stabilite în anexa la prezentul regulament.

Articolul 2

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în statele membre în conformitate cu tratatele.

Adoptat la Bruxelles, 28 iulie 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

([3]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANEXĂ

SPECIFICAȚII TEHNICE ALE SISTEMULUI INFORMATIC DESCENTRALIZAT

(menționate la articolul 1)

1. **Introducere și domeniu de aplicare**

Prezenta anexă stabilește specificațiile tehnice, măsurile și obiectivele sistemului informatic descentralizat pentru procedurile prevăzute în Regulamentul (UE) 2023/1543.

În conformitate cu Regulamentul (UE) 2023/1543, în special cu articolul 19, sistemul informatic descentralizat trebuie să permită comunicarea scrisă între autoritățile competente și sediile desemnate sau reprezentanții legali, între autoritățile competente, precum și între autoritățile competente și agențiile sau organele competente ale Uniunii.

2. **Definiții**

2.1. „protocol de transfer hipertext securizat" (*HyperText Transfer Protocol Secure*) sau „HTTPS" înseamnă canale de comunicații criptate și de conexiuni securizate;

2.2. „nerepudierea originii" înseamnă măsurile care furnizează dovada integrității și a originii datelor prin metode precum certificarea digitală, infrastructura de chei publice și semnăturile și sigiliile electronice;

2.3. „nerepudierea primirii informațiilor" înseamnă măsurile care îi furnizează emitentului dovada primirii informațiilor de către destinatarul vizat prin metode precum certificarea digitală, infrastructura de chei publice și semnăturile și sigiliile electronice;

2.4. „protocol simplu de acces la obiecte" (SOAP) înseamnă, în conformitate cu standardele consorțiului World Wide Web, o specificație a protocolului de mesagerie pentru schimbul de informații structurate cu privire la implementarea serviciilor web în rețelele informatice;

2.5. *Representational State Transfer* („REST") înseamnă un stil arhitectural pentru proiectarea aplicațiilor în rețea, care se bazează pe un model de comunicare apatridă client-server și care utilizează metode standard pentru efectuarea operațiunilor asupra resurselor, reprezentate de obicei în formate structurate;

2.6. „serviciu web" înseamnă un sistem software conceput pentru a permite interacțiunea interoperabilă între calculatoare în cadrul unei rețele și care are o interfață descrisă într-un format care poate fi prelucrat de un calculator;

2.7. „schimb de date" înseamnă schimbul de mesaje, formulare, documente și probe electronice prin intermediul sistemului informatic descentralizat;

2.8. „API" înseamnă o interfață de programare a aplicațiilor bazată pe un standard comun de schimb de date, care permite furnizorilor de servicii care utilizează soluții informatice personalizate în scopul schimbului de informații și de date legate de cererile de probe electronice să acceseze sistemele informatice descentralizate prin mijloace automatizate;

2.9. „interfață web" înseamnă o interfață cu utilizatorul disponibilă pe internet prin intermediul HTTPS, care le permite furnizorilor de servicii să acceseze manual sistemul informatic descentralizat pentru a comunica în condiții de siguranță cu autoritățile și pentru a face schimb de informații și date referitoare la cererile de probe electronice, fără a trebui să își stabilească o infrastructură proprie în acest scop;

2.10. „standarde ETSI" înseamnă specificațiile tehnice și standardele elaborate de Institutul European de Standardizare în Telecomunicații (ETSI) pentru a asigura interoperabilitatea, securitatea și eficiența tehnologiilor informației și comunicațiilor. Aceste standarde oferă cadre, protocoale și bune practici pentru o gamă largă de tehnologii, inclusiv rețele mobile, radiocomunicații, securitate cibernetică și infrastructură de internet;

2.11. „valoare de dispersie” înseamnă o ieșire cu lungime fixă generată de o funcție hash criptografică atunci când este aplicată la o intrare cu lungime arbitrară. O funcție hash criptografică este concepută pentru a îndeplini proprietățile fundamentale de securitate, inclusiv rezistența la preimagine, rezistența la preimagine secundară și rezistența la coliziune, asigurând robustețea acesteia împotriva inversiunii și a atacurilor de coliziune;

2.12. „sistem e-CODEX” înseamnă sistemul e-CODEX definit la articolul 3 alineatul (1) din Regulamentul (UE) 2022/850;

2.13. „Vocabularele de bază ale UE în domeniul e-justiției” înseamnă Vocabularele de bază ale UE în domeniul e-justiției, astfel cum sunt definite la punctul 4 din anexa la Regulamentul (UE) 2022/850;

2.14. „ebMS” înseamnă serviciul de mesagerie ebXML, care este un protocol de mesagerie dezvoltat în cadrul OASIS ce permite un schimb securizat, fiabil și interoperabil de documente comerciale electronice utilizând SOAP și care permite integrarea între întreprinderi în diferite sisteme;

2.15. „AS4” este abrevierea folosită pentru „*Applicability Statement 4*”, un standard OASIS care prezintă ebMS 3.0; acesta simplifică mesageria sigură și interoperabilă între întreprinderi prin utilizarea unor standarde deschise, cum ar fi SOAP și WS-Security;

2.16. Durata maximă de indisponibilitate înseamnă timpul maxim acceptabil până la restabilirea serviciului după un incident;

2.17. Pierderea de date maximă admisibilă înseamnă cantitatea maximă acceptabilă de pierderi de date în cazul unor defecțiuni.

3. **Metode de comunicare prin mijloace electronice**

3.1. În scopul comunicării scrise între autoritățile competente ale statelor membre, între autoritățile competente și sediile desemnate sau reprezentanții legali ai furnizorilor de servicii, precum și între autoritățile competente și agențiile sau organele Uniunii, sistemul informatic descentralizat utilizează metode de comunicare bazate pe servicii, cum ar fi serviciile web sau alte componente reutilizabile și soluții software pentru schimbul de date. Mai precis, aceasta va implica o comunicare prin intermediul punctelor de acces e-CODEX, astfel cum se prevede la articolul 5 alineatul (2) din Regulamentul (UE) 2022/850. Prin urmare, pentru a asigura un schimb transfrontalier de date eficace și interoperabil, sistemul informatic descentralizat permite comunicarea prin intermediul sistemului e-CODEX.

3.2. Având în vedere faptul că se preconizează un volum ridicat de probe electronice care vor fi transmise prin intermediul sistemului informatic descentralizat în urma unui ordin european de divulgare a probelor electronice, astfel cum se indică la articolul 19 alineatele (1) și (4) din Regulamentul (UE) 2023/1543, ceea ce poate duce la constrângeri ale capacității tehnice ce ar putea avea un impact negativ asupra sistemului informatic descentralizat, probele electronice se transmit prin intermediul acestui sistem în măsura în care acestea nu depășesc pragul de 25 de megabyți (25 600 de kilobyți). Transmiterea probelor electronice care depășesc pragul respectiv se efectuează în conformitate cu articolul 19 alineatul (5) din regulamentul respectiv.

3.3. Având în vedere articolul 19 alineatul (6) din Regulamentul (UE) 2023/1543, în cazul în care o transmitere se efectuează prin mijloace alternative, astfel cum se prevede la alineatul respectiv, ca urmare a incapacității de a utiliza sistemul informatic descentralizat din cauza unuia dintre motivele prevăzute la articolul 19 alineatul (5) din regulamentul respectiv:

3.3.1. În cazul în care transmiterea se referă la o comunicare scrisă, inclusiv la schimbul de formulare, între autoritățile competente și furnizorii de servicii în sensul articolului 19 alineatul (1) din Regulamentul (UE) 2023/1543, emitentul transmiterii înregistrează transmiterea în sistemul său informatic național care face parte din sistemul informatic descentralizat. Informațiile înregistrate includ cel puțin un număr de referință al cazului sau al fișierului, data și ora transmiterii, expeditorul și destinatarul, denumirea și dimensiunea fișierului.

3.3.2. În cazul în care transmiterea se referă la comunicarea scrisă, inclusiv la schimbul de formulare, între autoritățile competente, precum și la comunicarea scrisă cu agențiile sau organele competente ale Uniunii în sensul articolului 19 alineatul (4) din Regulamentul (UE) 2023/1543, emitentul transmiterii înregistrează transmiterea în sistemul informatic descentralizat, în special în cadrul sistemului său informatic național sau, după caz, în sistemele informatice gestionate de agenția sau organul competent al Uniunii. Informațiile înregistrate includ cel puțin un număr de referință al cazului sau al fișierului, data și ora transmiterii, expeditorul și destinatarul, denumirea și dimensiunea fișierului.

3.3.3. În cazul în care pentru transmiterea probelor electronice în temeiul unui ordin european de divulgare a probelor electronice s-au folosit mijloace alternative de comunicare între furnizorii de servicii și autoritățile competente din statul emitent ([1]) sau în cazul în care probele electronice sunt transmise prin mijloace alternative de la autoritatea de executare către autoritățile competente din statul emitent în cadrul procedurii de executare prevăzute la articolul 16 alineatul (9) din Regulamentul (UE) 2023/1543, emitentul:

(a) înregistrează și transmite autorității căreia i-au fost transmise sau puse la dispoziție probele electronice următoarele informații în cadrul unui manifest:

1. informații privind expeditorul și destinatarul;

2. metadatele care asociază probele electronice furnizate cu un anumit ordin european sau anumite ordine europene de divulgare sau de păstrare a probelor electronice;

3. data și ora transmiterii sau indicarea momentului în care probele electronice au fost puse la dispoziția destinatarului;

4. informații privind mijloacele de transmitere (de exemplu, o evidență a legăturii securizate prin care au fost puse la dispoziție probele electronice, dovada primirii sau a livrării de către serviciile poștale etc.) ([2]);

5. denumirea completă a fișierului care conține probele electronice transmise sau puse în alt mod la dispoziția destinatarului vizat din statul emitent;

6. dimensiunea datelor aferente probelor electronice transmise sau puse în alt mod la dispoziția destinatarului vizat din statul emitent;

7. cel puțin o valoare de dispersie a datelor care au fost transmise sau puse la dispoziție și o indicație a algoritmului sau algoritmilor hash utilizați. Algoritmul sau algoritmii hash utilizați pentru calcularea respectivei (respectivelor) valori de dispersie trebuie să fie puternic(i) din punct de vedere criptografic, utilizați la scară largă și să nu sufere de deficiențe care au fost făcute publice, cum ar fi coliziunile (de exemplu, SHA-512, SHA3-512, BLAKE2 sau RIPEMD-160, dar potențial mai puternice, în funcție de evoluțiile tehnologice);

(b) după caz, indică, în cadrul manifestului menționat la litera (a) de mai sus, data și ora până la care probele electronice vor rămâne accesibile. Acest termen oferă autorității competente din statul emitent un interval de timp rezonabil pentru a recupera probele electronice, care nu poate fi mai mic de 10 zile calendaristice și mai mare de 45 de zile calendaristice din momentul în care au fost puse la dispoziție probele electronice. La cererea autorității competente a statului emitent, termenul indicat de emitent poate fi prelungit într-un caz individual;

(c) poate înregistra și transmite informații sau observații suplimentare relevante pentru caz autorității căreia i-au fost transmise sau puse la dispoziție probele electronice, în cadrul manifestului menționat la litera (a) de mai sus.

3.4. Având în vedere articolul 28 din Regulamentul (UE) 2023/1543, software-ul de implementare de referință colectează, transmite sau oferă în alt mod acces, în mod automat, la statisticile menționate la alineatul (2) de la articolul respectiv atât în formate de date structurate (de exemplu, XML), cât și în formate nestructurate (de exemplu, PDF). În conformitate cu articolul 28 alineatul (3) din Regulamentul (UE) 2023/1543, în cazul în care sunt echipate din punct de vedere tehnic, portalurile naționale ([3]) gestionate de statele membre pot, de asemenea, să transmită sau să furnizeze aceste statistici Comisiei printr-un proces automatizat. Comisia emite orientări privind structura datelor și metoda de colectare și comunicare a acestor statistici.

([1]) Pentru mai multă claritate, trimiterile la autoritățile naționale competente se interpretează, *mutatis mutandis*, ca aplicându-se membrilor naționali ai Eurojust, procurorilor europeni și procurorilor europeni delegați, în măsura în care aceștia sunt împuterniciți să îndeplinească aceleași funcții atât în temeiul dreptului UE, cât și al dreptului intern.

([2]) Ar trebui reamintit faptul că, în conformitate cu articolul 19 alineatul (5), transmiterea prin astfel de mijloace alternative de comunicare trebuie să îndeplinească cerințele de a fi rapidă, sigură și fiabilă, permițând destinatarului să stabilească autenticitatea.

([3]) „Portalurile naționale” ar trebui înțelese ca fiind „sisteme informatice” naționale care fac parte din sistemul informatic descentralizat, astfel cum este definit la articolul 3 punctul 21 din Regulamentul (UE) 2023/1543.

4. **Protocoale de comunicare**

4.1. Sistemul informatic descentralizat utilizează protocoale de internet securizate pentru:

(a) comunicarea în cadrul sistemului informatic descentralizat între autoritățile competente;

(b) comunicarea în cadrul sistemului informatic descentralizat între autoritățile competente și agențiile și organele Uniunii;

(c) comunicarea între autoritățile competente și furnizorii de servicii prin intermediul unei API și al interfeței web și

(d) comunicarea cu baza de date a Curții.

4.2. Pentru definirea și transmiterea datelor și metadatelor structurate, componentele sistemului informatic descentralizat se bazează pe standarde și protocoale industriale cuprinzătoare și general acceptate, cum ar fi SOAP și REST, în special cele nominalizate de organizațiile de standardizare europene precum ETSI.

4.3. În ceea ce privește protocoalele de transport și mesagerie, sistemul informatic descentralizat se bazează pe protocoale securizate bazate pe standarde, cum ar fi:

(a) profilul AS4 pentru schimbul transfrontalier de date, care asigură transmiterea de mesaje sigure și fiabile cu criptare și nerepudiere;

(b) API-uri RESTful/HTTPS pentru comunicare, care suportă formatele JSON și XML;

(c) SOAP pentru interacțiuni de înaltă fiabilitate, care încorporează WS-Security pentru autentificare și criptare.

4.4. În scopul schimbului neîntrerupt și interoperabil de date, protocoalele de comunicare utilizate de sistemul informatic descentralizat respectă standardele de interoperabilitate relevante.

4.5. După caz, schemele XML pentru probele electronice utilizează standardele sau vocabularele relevante, care sunt necesare pentru validarea corespunzătoare a elementelor și tipurilor definite în cadrul acestei scheme. Printre acestea se numără:

(a) vocabularul de bază al UE în domeniul e-justiției;

(b) tipurile de date necalificate;

(c) o listă de coduri pentru codurile lingvistice ale Uniunii Europene.

De asemenea, după caz, schemele XML pot include standarde ETSI relevante pentru a utiliza definițiile acestora.

4.6. Comisia definește specificațiile API comune, care sunt puse la dispoziția furnizorilor de servicii de către statele de executare, ca mijloc de accesare a sistemului informatic descentralizat. În măsura în care acest lucru este posibil și rezonabil, această API se bazează pe standardul ETSI TS 104 144 [„Definiția interfeței în sensul Regulamentului (UE) 2023/1543 privind probele electronice pentru autoritățile naționale și furnizorii de servicii”].

4.7. În ceea ce privește protocoalele de securitate și autentificare, sistemul informatic descentralizat se bazează pe protocoale bazate pe standarde, cum ar fi:

(a) TLS (*Transport Layer Security* – securitatea pe nivelul de transport) pentru comunicarea criptată și autentificată prin rețele, care permite autentificarea reciprocă prin intermediul certificatelor digitale X.509;

(b) *OAuth*/*OpenID Connect* (OIDC) pentru autentificarea și autorizarea securizată;

(c) infrastructura de chei publice (PKI – *Public Key Infrastructure*) și semnăturile digitale pentru schimbul securizat de chei și verificarea integrității mesajelor, care utilizează certificate digitale (X.509) emise de autorități de certificare (AC) de încredere.

5. **Obiective de securitate a informațiilor și măsuri tehnice relevante**

5.1. În ceea ce privește schimbul de informații prin intermediul sistemului informatic descentralizat, printre măsurile tehnice de asigurare a standardelor minime de securitate informatică se numără:

(a) măsuri care să asigure confidențialitatea informațiilor, inclusiv prin utilizarea unor canale securizate de comunicare;

(b) măsuri care să asigure integritatea datelor (mesaje, formulare, documente și probe electronice) în repaus și în tranzit;

(c) măsuri care să asigure nerepudierea originii expeditorului informațiilor în cadrul sistemului informatic descentralizat și nerepudierea primirii informațiilor;

(d) măsuri care să asigure disponibilitatea prin asigurarea accesului permanent la servicii și date, prevenind perturbările cauzate de atacuri cibernetice sau defecțiuni;

(e) măsuri care să asigure păstrarea evidenței evenimentelor care ar putea compromite securitatea informațiilor, în conformitate cu recomandările internaționale recunoscute pentru standardele de securitate informatică;

(f) măsuri care să asigure autentificarea și autorizarea utilizatorilor și măsuri de verificare a identității sistemelor conectate la sistemul informatic descentralizat.

5.2. Componentele sistemului informatic descentralizat asigură comunicarea și transmiterea securizată a datelor, utilizând criptarea, infrastructura de chei publice cu certificate digitale pentru autentificare și schimbul securizat de chei, precum și protocoale de mesagerie securizată, cum ar fi AS4 (ebMS), API RESTful și SOAP, în vederea păstrării confidențialității și integrității mesajelor.

5.3. Componentele sistemului informatic descentralizat sunt dezvoltate în conformitate cu principiul protecției datelor începând cu momentul conceperii și în mod implicit și se pun în aplicare măsuri administrative, organizatorice și tehnice adecvate pentru a asigura un nivel ridicat de securitate cibernetică.

5.4. Comisia proiectează, dezvoltă și întreține software-ul de implementare de referință în conformitate cu cerințele și principiile privind protecția datelor prevăzute în Regulamentul (UE) 2018/1725. Software-ul de implementare de referință furnizat de Comisie permite statelor membre să își respecte obligațiile care le revin în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului ([4]) și, respectiv, al Directivei (UE) 2016/680 a Parlamentului European și a Consiliului ([5]), după caz.

5.5. Statele membre care utilizează un sistem informatic național diferit de software-ul de implementare de referință pun în aplicare măsurile necesare pentru a se asigura că acesta respectă cerințele Regulamentului (UE) 2016/679 și ale Directivei (UE) 2016/680, după caz.

5.6. Având în vedere participarea lor la sistemul informatic descentralizat, Eurojust și Parchetul European pun în aplicare măsurile necesare pentru a se asigura că sistemele lor informatice respectă cerințele Regulamentului (UE) 2018/1725 și ale actelor lor de instituire.

5.7. Pentru sistemele informatice aflate în responsabilitatea lor care fac parte din sistemul informatic descentralizat, statele membre, Eurojust și Parchetul European instituie mecanisme solide de detectare a amenințărilor și de răspuns la incidente cibernetice cu scopul de a asigura identificarea și atenuarea incidentelor de securitate cibernetică și restabilirea în timp util a serviciului în urma acestora, în conformitate cu politicile lor relevante.

6. **Criptarea probelor electronice** ([6])

6.1. Fără a aduce atingere măsurilor de securitate prevăzute de sistemul informatic descentralizat, atunci când emit un ordin european de divulgare a probelor electronice, autoritățile competente pot furniza, în plus, un certificat public specific X.509 pentru criptarea asimetrică a probelor electronice.

([4]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([5]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

([6]) Pentru eliminarea oricărei ambiguități, termenul „probe electronice” se limitează la definiția prevăzută la articolul 3 alineatul (8) din Regulamentul (UE) 2023/1543.

6.2. Emiterea, gestionarea, verificarea și toate aspectele conexe ale certificatelor menționate la punctul 6.1, împreună cu infrastructura de chei publice corespunzătoare, sunt responsabilitatea exclusivă a statului emitent.

6.3. Fără a aduce atingere evoluțiilor tehnologice viitoare, certificatele publice permit utilizarea algoritmilor de criptare standard din industrie, cum ar fi RSA (*Rivest-Shamir-Adleman*) sau ECDH (*Elliptic Curve Diffie-Hellman*) pentru ECC (criptografia bazată pe curbe eliptice).

6.4. Certificatele publice trebuie să conțină extensia „keyUsage" corespunzătoare, cum ar fi „keyEncipherment" sau „dataEncipherment" pentru certificatele bazate pe RAS și „keyAgreement" pentru certificatele bazate pe ECC. Certificatele trebuie puse la dispoziție în format PEM (*Privacy-Enhanced Mail* – mesagerie electronică cu confidențialitate sporită) sau DER (reguli de codificare diferențiate).

6.5. În cazul în care autoritatea emitentă a furnizat un certificat public X.509, iar un furnizor de servicii trimite probele electronice care urmează să fie divulgate în temeiul unui ordin european de divulgare a probelor electronice, furnizorul, înainte să transmită datele respective prin intermediul sistemului informatic descentralizat, criptează probele electronice utilizând respectivul certificat public X.509 furnizat de statul emitent.

6.6. În cazul în care autoritatea emitentă a furnizat un certificat public X.509, dar transmiterea probelor electronice în formă criptată nu este posibilă din motive tehnice sau din alte motive justificate, și fără a aduce atingere dispoziției prevăzute la articolul 19 alineatul (5) din Regulamentul (UE) 2023/1543, furnizorul de servicii poate transmite datele fără criptarea conținutului. În astfel de cazuri, furnizorul de servicii oferă autorității emitente o explicație motivată.

7. **Obiective minime de disponibilitate**

7.1. Statele membre, Eurojust și Parchetul European asigură disponibilitatea componentelor sistemului informatic descentralizat aflate în responsabilitatea lor 24 de ore din 24, șapte zile din șapte, cu o rată țintă de disponibilitate tehnică de cel puțin 98 % pe an, cu excepția operațiunilor de întreținere programate.

7.2. Comisia asigură disponibilitatea bazei de date a Curții 24 de ore din 24, șapte zile din șapte, cu o rată țintă de disponibilitate tehnică de peste 99 % pe an, cu excepția operațiunilor de întreținere programate.

7.3. În măsura în care este posibil, în zilele lucrătoare, operațiunile de întreținere trebuie să fie planificate în intervalul 20:00-7:00 CET.

7.4. Statele membre, Eurojust și Parchetul European notifică Comisiei și celorlalte state membre activitățile de întreținere după cum urmează:

(a) cu 5 zile lucrătoare înainte pentru operațiunile de întreținere care pot duce la o perioadă de indisponibilitate de până la 4 ore;

(b) cu 10 zile lucrătoare înainte pentru operațiunile de întreținere care pot duce la o perioadă de indisponibilitate cuprinsă între 4 și 12 ore;

(c) cu 30 de zile lucrătoare înainte pentru operațiunile de întreținere care pot duce la o perioadă de indisponibilitate de peste 12 ore.

7.5. În cazul în care statele membre, Eurojust sau Parchetul European au stabilit ferestre de întreținere periodică, acestea informează Comisia și participanții la sistemul informatic descentralizat cu privire la ora și ziua (zilele) în care sunt planificate astfel de ferestre fixe de întreținere periodică. Fără a aduce atingere obligațiilor prevăzute la punctul 7.4, în cazul în care componentele sistemului informatic descentralizat aflate în responsabilitatea statelor membre, a Eurojust sau a Parchetului European devin indisponibile în timpul unei astfel de ferestre fixe de întreținere periodică, acestea pot alege să nu notifice acest lucru Comisiei de fiecare dată.

7.6. În cazul unei defecțiuni tehnice neprevăzute a componentelor sistemului informatic descentralizat aflate în responsabilitatea statelor membre, a Eurojust sau a Parchetului European, acestea informează fără întârziere Comisia și participanții la sistemul informatic descentralizat cu privire la această defecțiune, precizând și intervalul de timp preconizat pentru restabilirea serviciului, dacă acesta se cunoaște.

7.7. În cazul unor activități de întreținere sau al unor defecțiuni tehnice neprevăzute ale componentelor sistemului informatic descentralizat aflate în responsabilitatea unui stat membru, care au un impact negativ asupra disponibilității API și/sau a interfeței web pentru furnizorii de servicii, statul membru în cauză pune prompt la dispoziție aceste informații pe un site web și/sau le comunică furnizorilor de servicii care își desfășoară activitatea pe teritoriul său, fără întârzieri nejustificate.

7.8. În cazul unei defecțiuni tehnice neprevăzute a bazei de date a Curții, Comisia informează fără întârziere statele membre, Eurojust și Parchetul European cu privire la această indisponibilitate, precizând și intervalul de timp preconizat pentru restabilirea serviciului, dacă acesta se cunoaște.

7.9. În cazul unei întreruperi a serviciului, statele membre, Eurojust și Parchetul European asigură restabilirea rapidă a serviciului și o pierdere minimă de date, în conformitate cu durata maximă de indisponibilitate și cu pierderea de date maximă admisibilă.

7.10. Statele membre, Eurojust și Parchetul European pun în aplicare măsuri adecvate pentru a atinge obiectivele de disponibilitate prezentate anterior și stabilesc proceduri pentru a răspunde în mod eficace la incidentele cibernetice.

8. **Baza de date a autorităților competente/Curții (BDC)**

8.1. Având în vedere articolul 19 din Regulamentul (UE) 2023/1543, în scopul funcționării sistemului informatic descentralizat, este esențial să se creeze o bază de date oficială a furnizorilor de servicii și a autorităților competente.

8.2. Baza de date oficială a autorităților competente conține următoarele informații într-un format structurat:

(a) în sensul articolului 19 din Regulamentul (UE) 2023/1543, informații privind autoritățile competente notificate în temeiul articolului 31 alineatul (1) literele (a)-(c) din regulamentul respectiv, inclusiv cu privire la:

1. membrii naționali ai Eurojust, împreună cu o indicație a faptului că aceștia sunt sau nu autorizați, în temeiul dreptului național, să emită ordine europene de divulgare și ordine europene de păstrare a probelor electronice în conformitate cu articolul 8 alineatele (3) și (4) din Regulamentul (UE) 2018/1727 al Parlamentului European și al Consiliului ([7]).

2. procurorii europeni delegați și procurorii europeni, în cazul în care sunt notificați de statele membre în conformitate cu articolul 105 alineatul (3) din Regulamentul (UE) 2017/1939 ([8]) al Consiliului în calitate de autoritate emitentă competentă în sensul Regulamentului (UE) 2023/1543;

(b) după caz, informațiile necesare pentru a stabili zonele geografice de competență ale autorităților sau alte criterii relevante necesare pentru stabilirea competenței acestora;

(c) informațiile necesare pentru funcționarea corectă a schimburilor de date și direcționarea (rutarea) mesajelor tehnice ale unor astfel de schimburi în cadrul sistemului informatic descentralizat.

8.2.1. Informațiile menționate la punctul 8.2 litera (c) includ următoarele:

(a) informații privind statul membru în care este stabilit sediul desemnat al furnizorului de servicii sau în care își are reședința reprezentantul legal al acestuia:

1. statul membru;

2. autoritatea centrală;

([7]) Regulamentul (UE) 2018/1727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului (JO L 295, 21.11.2018, p. 138).

([8]) Regulamentul (UE) 2017/1939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO) (JO L 283, 31.10.2017, p. 1).

(b) informații privind furnizorul de servicii:

1. numele/denumirea;
2. adresa/sediul social;
3. numărul de înregistrare;
4. forma juridică;
5. numărul de telefon;
6. adresa de e-mail;

(c) informații privind sediul desemnat/reprezentantul legal:

1. tipul de entitate (sediu desemnat/reprezentant legal);
2. numele/denumirea;
3. adresa/sediul social;
4. numărul de telefon;
5. adresa de e-mail;
6. persoana/entitatea de contact pentru situații generale;
7. limba sau limbile oficiale acceptate de furnizorul de servicii/sediul desemnat/reprezentantul legal;
8. serviciile menționate la articolul 2 alineatul (1) din Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului ([9]), care sunt oferite în Uniune;
9. tipul de instrumente juridice ale UE pentru care se desemnează sediul desemnat/reprezentantul legal (în situațiile în care statele membre nu participă la toate instrumentele juridice relevante ale UE);
10. domeniul de aplicare teritorială a desemnării/numirii;

(d) autentificarea informațiilor:

1. numele reprezentantului autorizat;
2. funcția ocupată;
3. adresa;
4. numărul de telefon;
5. adresa de e-mail;
6. data.

8.2.2. În cazul în care sunt disponibile, informațiile menționate la punctul 8.2 litera (c) pot include:

(a) informații privind furnizorul de servicii:

1. persoana de contact pentru întrebări privind notificările (dacă aceasta este diferită de semnatar);
2. site-ul web;

(b) tipuri de date disponibile:

1. pentru fiecare serviciu vizat:

— tipurile de date disponibile;

— categoria de date;

— identificatorii;

— perioada de disponibilitate a datelor;

([9]) Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului din 12 iulie 2023 de stabilire a unor norme armonizate privind desemnarea sediilor desemnate și numirea reprezentanților legali în scopul obținerii de probe electronice în cadrul procedurilor penale (JO L 191, 28.7.2023, p. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2. informații suplimentare privind datele;

3. informații suplimentare privind serviciul (de exemplu, relațiile de subcontractare);

(c) informații privind sediul desemnat/reprezentantul legal:

1. alți furnizori de servicii pentru care se desemnează sediul desemnat sau reprezentantul legal;

2. datele de contact pentru asistență tehnică;

3. persoana de contact pentru situații de urgență;

(d) informații tehnice:

1. denumirea punctului de contact tehnic;

2. numărul de telefon al punctului de contact tehnic;

3. adresa de e-mail a punctului de contact tehnic;

4. URL-ul API pentru extragerea dinamică a informațiilor privind tipurile de date;

5. tipul de conexiune la sistemul informatic național:

— interfața web;

— API;

— URL-ul API push.

8.3. Având în vedere nevoile operaționale ale sistemului informatic descentralizat:

(a) Comisia este responsabilă cu dezvoltarea, întreținerea, operarea și sprijinirea bazei de date oficiale;

(b) Comisia face posibil accesul la baza de date oficială prin intermediul unei API puse la dispoziția autorităților competente, a Eurojust și a Parchetului European în scopul participării acestora la sistemul informatic descentralizat;

(c) statele membre se asigură că informațiile privind autoritățile lor competente, prevăzute la punctul 8.2 literele (a) și (b) și incluse în baza de date oficială, sunt complete, exacte și actualizate;

(d) baza de date oficială le permite statelor membre să furnizeze și să actualizeze, în cadrul acesteia, informațiile privind furnizorii lor de servicii, iar autorităților care participă la sistemul informatic descentralizat să acceseze și să extragă în mod automat informațiile respective;

(e) statele membre și furnizorii de servicii se asigură că informațiile prevăzute la punctul 8.2 litera (c) și incluse în baza de date oficială sunt complete, exacte și actualizate.