REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/2447 AL COMISIEI

din 4 decembrie 2025

de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1727 al Parlamentului European și al Consiliului în ceea ce privește specificațiile tehnice, măsurile și alte cerințe pentru instituirea și utilizarea sistemului informatic descentralizat pentru prelucrarea și comunicarea securizate ale informațiilor

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 ([1]), în special articolul 22a alineatul (3) și articolul 22b alineatul (1) literele (a), (b), (c) și (d),

întrucât:

(1) Regulamentul (UE) 2018/1727 stabilește cadrul pentru noua infrastructură digitală internă a Eurojust și pentru instituirea unui sistem descentralizat și securizat de comunicații digitale între autoritățile naționale competente ale statelor membre și Eurojust.

(2) Comunicațiile digitale securizate se realizează prin intermediul sistemului informatic descentralizat. Pentru instituirea sistemului informatic descentralizat, este necesar să se stabilească specificații tehnice care să definească metodele și protocoalele de comunicație, măsuri tehnice care să asigure standarde minime în materie de securitate a informațiilor și de securitate, precum și obiective de disponibilitate minimă pentru implementarea sistemului respectiv.

(3) În conformitate cu articolul 22a alineatul (1) din Regulamentul (UE) 2018/1727, sistemul informatic descentralizat va fi alcătuit din sistemele informatice ale statelor membre și ale Eurojust și din puncte de acces e-CODEX interoperabile prin care sistemele informatice respective să fie interconectate. Specificațiile tehnice și alte cerințe ale sistemului informatic descentralizat prevăzute în prezentul regulament ar trebui să țină seama de cadrul respectiv.

(4) 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]).

(5) Sistemul informatic descentralizat este implementat în cadrul unui sistem informatic descentralizat mai mare, bazat pe e-CODEX, denumit Sistemul de schimb digital în domeniul justiției (JUDEX). Prin urmare, este necesar să se asigure un schimb eficace de informații privind evoluțiile orizontale.

(6) În conformitate cu articolul 22a alineatul (4) din Regulamentul (UE) 2018/1727, statele membre și Eurojust 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.

(7) Datele referitoare la infracțiunile de terorism și la formele grave de criminalitate organizată ar trebui transmise într-un mod structurat pentru a îmbunătăți calitatea și relevanța informațiilor, precum și pentru a se asigura că informațiile pot fi integrate mai eficient în sistemul Eurojust de gestionare a cazurilor și pot fi comparate mai bine cu informațiile deja stocate în sistemul respectiv. În ceea ce privește datele dactiloscopice și fotografiile, care pot fi transmise către Eurojust în scopul identificării persoanelor care fac obiectul procedurilor penale legate de infracțiuni de terorism, ar trebui definite formatul și standardele tehnice pentru transmitere.

([1]) JO L 295, 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/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).

(8) Eurojust facilitează și sprijină emiterea și executarea cererilor de cooperare judiciară, inclusiv a cererilor și a deciziilor bazate pe instrumentele de punere în aplicare a principiului recunoașterii reciproce. Autoritățile naționale competente ar trebui să poată solicita asistență și coordonare din partea Eurojust prin intermediul sistemului informatic descentralizat.

(9) Pentru a se asigura eficiența și consecvența, este important ca specificațiile tehnice care urmează să fie stabilite în temeiul Regulamentului (UE) 2018/1727 să fie compatibile cu specificațiile tehnice stabilite în temeiul Regulamentelor (UE) 2023/2844 ([3]), (UE) 2023/1543 ([4]) și (UE) 2024/3011 ([5]) ale Parlamentului European și ale Consiliului, precum și cu viitoarele măsuri de digitalizare relevante pentru mandatul Eurojust de a sprijini autoritățile naționale competente.

(10) Orice altă comunicare între Eurojust și autoritățile naționale competente, cum ar fi comunicarea de informații privind rezultatele prelucrării informațiilor, inclusiv existența unor legături cu cazurile deja stocate în sistemul de gestionare a cazurilor în conformitate cu articolul 22 din Regulamentul (UE) 2018/1727, atunci când Eurojust acționează din proprie inițiativă, sau de informații transmise Eurojust în scopul conservării, analizării și stocării probelor legate de genocid, de crime împotriva umanității, de crime de război și de infracțiuni conexe în conformitate cu articolul 4 alineatul (1) litera (j) din regulamentul respectiv, ar trebui, de asemenea, să fie permisă prin intermediul sistemului informatic descentralizat.

(11) Pentru a se asigura că prezentul regulament ține seama de nevoile operaționale ale Eurojust, agenția a fost consultată în conformitate cu articolul 22a alineatul (3) din Regulamentul (UE) 2018/1727.

(12) În conformitate cu articolul 4 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Irlanda și-a notificat, prin scrisoarea din 9 septembrie 2019, intenția de a accepta Regulamentul (UE) 2018/1727 și de a-și asuma obligații în temeiul acestuia. Decizia (UE) 2019/2006 a Comisiei ([6]) a confirmat participarea menționată. Regulamentul (UE) 2023/2131 al Parlamentului European și al Consiliului ([7]) a modificat Regulamentul (UE) 2018/1727 pentru a permite instituirea unor canale de comunicare digitală securizate între Eurojust și autoritățile naționale competente și pentru a oferi temeiul juridic pentru prezentul regulament. În situațiile în care Irlanda nu și-a notificat intenția de a participa la adoptarea și aplicarea Regulamentului (UE) 2023/2131 și nici intenția de a accepta regulamentul respectiv și de a-și asuma obligații în temeiul acestuia, Irlanda, în conformitate cu articolele 1 și 2 și cu articolul 4a alineatul (1) din Protocolul nr. 21, nu are obligații în temeiul Regulamentului (UE) 2023/2131 și nici nu face obiectul aplicării acestuia. Prin urmare, Irlanda nu participă la adoptarea prezentului regulament.

(13) 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, Danemarca nu a participat la adoptarea Regulamentului (UE) 2018/1727. Prin urmare, Danemarca nu are obligații în temeiul prezentului regulament și nu face obiectul aplicării acestuia.

([3]) Regulamentul (UE) 2023/2844 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind digitalizarea cooperării judiciare și a accesului la justiție în cadrul procedurilor transfrontaliere în materie civilă, comercială și penală și de modificare a anumitor acte din domeniul cooperării judiciare (JO L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

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

([5]) Regulamentul (UE) 2024/3011 al Parlamentului European și al Consiliului din 27 noiembrie 2024 privind transferul procedurilor în materie penală (JO L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Decizia (UE) 2019/2006 a Comisiei din 29 noiembrie 2019 privind participarea Irlandei la Regulamentul (UE) 2018/1727 al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) (JO L 310, 2.12.2019, p. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Regulamentul (UE) 2023/2131 al Parlamentului European și al Consiliului din 4 octombrie 2023 de modificare a Regulamentului (UE) 2018/1727 al Parlamentului European și al Consiliului și a Deciziei 2005/671/JAI a Consiliului în ceea ce privește schimbul de informații digitale în cazurile de terorism (JO L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) 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 ([8]) și a emis un aviz la 21 octombrie 2025.

(15) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit în temeiul articolului 22c din Regulamentul (UE) 2018/1727,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Specificații tehnice ale sistemului informatic descentralizat

Specificațiile tehnice, măsurile și obiectivele sistemului informatic descentralizat menționate la articolul 22b alineatul (1) literele (a), (b), (c) și (d) din Regulamentul (UE) 2018/1727 sunt stabilite în anexa I la prezentul regulament.

Articolul 2

Standarde procedurale digitale

Standardele procedurale digitale aplicabile comunicațiilor electronice prin intermediul sistemului informatic descentralizat menționate la articolul 22a alineatul (3) din Regulamentul (UE) 2018/1727 sunt stabilite în anexa II la prezentul regulament.

Articolul 3

Specificații tehnice pentru transmiterea amprentelor digitale și a fotografiilor

Specificațiile tehnice și formatul pentru transmiterea amprentelor digitale și a fotografiilor, ~~astfel~~ cum se menționează la articolul 22a alineatul (3) din Regulamentul (UE) 2018/1727, sunt stabilite în anexa III la prezentul regulament.

Articolul 4

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, 4 decembrie 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

([8]) 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).

ANEXA I

SPECIFICAȚIILE TEHNICE, MĂSURILE ȘI OBIECTIVELE SISTEMULUI INFORMATIC DESCENTRALIZAT

1. **Introducere și domeniu de aplicare**

Prezenta anexă stabilește specificațiile tehnice, măsurile și obiectivele sistemului informatic descentralizat pentru schimbul de informații în temeiul Regulamentului (UE) 2018/1727.

Caracterul descentralizat al sistemului informatic permite schimbul de date în mod direct și securizat între autoritățile naționale competente și Eurojust.

2. **Definiții**

În sensul prezentei anexe, se aplică următoarele 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, semnăturile și sigiliile electronice;

2.4. „SOAP” (*Simple Object Access Protocol* – protocol simplu de acces la obiecte) 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. „REST” (*Representational State Transfer*) 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 și de documente prin intermediul sistemului informatic descentralizat;

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

2.9. „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;

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

2.11. „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;

2.12. „obiectiv privind timpul de recuperare” înseamnă timpul maxim acceptabil până la restabilirea serviciului după un incident;

2.13. „obiectiv privind punctul de recuperare” înseamnă cantitatea maximă acceptabilă de pierderi de date în cazul unor defecțiuni.

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

3.1. Sistemul informatic descentralizat utilizează metode de comunicare bazate pe servicii, cum ar fi serviciile web sau alte componente și soluții software reutilizabile, în scopul schimbului de mesaje și documente.

3.2. Mai precis, sistemul informatic descentralizat implică comunicarea 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.

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 și Eurojust;

(b) comunicarea cu baza de date a autorității competente/Curții, astfel cum se menționează la punctul 7.1.

4.2. Pentru definirea și transmiterea datelor și a metadatelor structurate, componentele sistemului informatic descentralizat se bazează pe standarde și protocoale industriale cuprinzătoare și general acceptate, cum ar fi SOAP și REST.

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 utilizează standardele sau vocabularele relevante, care sunt necesare pentru validarea corespunzătoare a elementelor și tipurilor definite în cadrul acestei scheme. Aceste standarde sau vocabulare pot include:

(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.

4.6. 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) PKI (*Public Key Infrastructure* – infrastructura de chei publice) 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 și următoarele:

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

(b) măsuri care să asigure integritatea datelor 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 păstrarea evidenței evenimentelor care ar putea compromite securitatea informațiilor, în conformitate cu recomandările internaționale recunoscute pentru standardele de securitate informatică ([1]);

(e) 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. În cazul în care se utilizează TLS în contextul sistemului informatic descentralizat, se va utiliza cea mai recentă versiune stabilă a protocolului sau, în lipsa acesteia, o versiune fără vulnerabilități de securitate cunoscute. Sunt permise numai lungimi ale cheilor care asigură un nivel adecvat de securitate criptografică și nu se vor utiliza suite de cifrare cunoscute ca fiind nesigure sau învechite.

5.4. În măsura posibilului, certificatele digitale PKI utilizate în scopul funcționării sistemului informatic descentralizat sunt eliberate de autoritățile de certificare recunoscute ca prestatori de servicii de încredere calificați în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([2]). Se pun în aplicare măsuri pentru a se asigura că astfel de certificate sunt utilizate exclusiv în scopurile pentru care au fost concepute, la nivelul necesar de încredere și în conformitate cu cerințele aplicabile din Regulamentul (UE) nr. 910/2014.

5.5. 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.

5.6. 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 ([3]) și, respectiv, al Directivei (UE) 2016/680, după caz.

([1]) Fără a aduce atingere înregistrării în scopuri de securitate, mecanismele de înregistrare utilizate de componentele sistemului informatic descentralizat permit, după caz, asigurarea conformității cu cerințele prevăzute la articolul 88 din Regulamentul (UE) 2018/1725 și, după caz, la articolul 25 din 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

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

5.8. Eurojust pune în aplicare măsurile necesare pentru a se asigura că sistemul său back-end sau o instanță a software-ului de implementare de referință pe care îl utilizează respectă cerințele Regulamentelor (UE) 2018/1725 și (UE) 2018/1727.

5.9. Pentru sistemele informatice aflate în responsabilitatea lor care fac parte din sistemul informatic descentralizat, statele membre și Eurojust 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. **Obiective minime de disponibilitate**

6.1. Eurojust și statele membre 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.

6.2. 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.

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

6.4. Statele membre notifică Comisiei, Eurojust 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.

6.5. În cazul în care statele membre au stabilit ferestre de întreținere periodică, acestea informează Comisia, Eurojust și celelalte state membre cu privire la ora și ziua (zilele) în care sunt planificate astfel de ferestre fixe de întreținere periodică. Prin derogare de la obligațiile prevăzute în teza 1, în cazul în care componentele sistemului informatic descentralizat aflate sub responsabilitatea statelor membre devin indisponibile într-o astfel de fereastră fixă de întreținere periodică, statele membre pot alege să nu notifice Comisia de fiecare dată.

6.6. În cazul unei defecțiuni tehnice neprevăzute a unei componente a sistemului informatic descentralizat aflate în responsabilitatea statelor membre, acestea din urmă informează fără întârziere Comisia și celelalte state membre cu privire la defecțiune, precizând și intervalul de timp preconizat pentru restabilirea serviciului, dacă acesta se cunoaște.

6.7. Eurojust notifică Comisiei și statelor 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.

6.8. În cazul în care Eurojust a stabilit ferestre de întreținere periodică, Eurojust informează Comisia și statele membre cu privire la ora și ziua (zilele) în care sunt planificate astfel de ferestre fixe de întreținere periodică. Prin derogare de la obligațiile prevăzute la prima teză, în cazul în care componentele sistemului informatic descentralizat aflate sub responsabilitatea Eurojust devin indisponibile într-o astfel de fereastră fixă de întreținere periodică, Eurojust poate alege să nu notifice Comisia de fiecare dată.

6.9. În cazul unei defecțiuni tehnice neprevăzute a unei componente a sistemului informatic descentralizat aflate în responsabilitatea Eurojust, acesta din urmă informează fără întârziere Comisia și statele membre cu privire la defecțiune, precizând și intervalul de timp preconizat pentru restabilirea serviciului, dacă acesta se cunoaște.

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

6.11. În cazul unei întreruperi a serviciului, statele membre și Eurojust asigură restabilirea rapidă a serviciului și o pierdere minimă de date, în conformitate cu obiectivul privind timpul de recuperare și obiectivul privind punctul de recuperare.

6.12. Statele membre și Eurojust pun în aplicare măsuri adecvate pentru atingerea obiectivelor de disponibilitate prezentate anterior și stabilesc proceduri pentru a răspunde în mod eficace la incidentele cibernetice.

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

7.1. În temeiul articolului 22a din Regulamentul (UE) 2018/1727, sistemul informatic descentralizat permite comunicația electronică între autoritățile naționale competente și Eurojust. Având în vedere obligațiile privind schimbul de informații între autoritățile naționale competente și Eurojust în temeiul articolelor 21, 21a și 22, dar și rolul Eurojust în facilitarea și sprijinirea emiterii și executării oricărei cereri de asistență judiciară reciprocă sau de recunoaștere reciprocă în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2018/1727, autoritățile competente implicate trebuie să fie clar identificabile atunci când utilizează sistemul informatic descentralizat. Prin urmare, este esențial să se creeze o bază de date oficială cu informațiile acestor autorități în scopuri legate de funcționarea sistemului informatic descentralizat.

7.2. BDC trebuie să includă următoarele informații într-un format structurat:

(a) în sensul articolului 8 alineatul (1), al articolului 8 alineatul (3), al articolului 8 alineatul (4), al articolului 21, al articolului 21a și al articolului 22 din Regulamentul (UE) 2018/1727, informații privind autoritățile naționale competente, inclusiv corespondenții naționali, astfel cum se prevede la articolul 20 din regulamentul respectiv, precum și membrii naționali în conformitate cu articolul 7 ([4]) din regulamentul respectiv;

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

(c) informațiile necesare pentru direcționarea corectă a mesajelor tehnice în cadrul sistemului informatic descentralizat.

7.3. Comisia este responsabilă cu dezvoltarea, întreținerea, operarea și sprijinirea BDC.

7.4. BDC permite statelor membre și Eurojust să actualizeze informațiile conținute, iar autorităților naționale competente și membrilor naționali care participă la sistemul informatic descentralizat, să acceseze și să extragă în mod programat informațiile conținute.

7.5. Accesul la BDC este posibil prin intermediul unui protocol comun de comunicare, indiferent dacă autoritățile competente conectate la sistemul informatic descentralizat operează un sistem back-end național sau o versiune a software-ului de implementare de referință.

7.6. Statele membre se asigură că informațiile privind autoritățile lor competente din BDC, astfel cum se prevede la punctul 7.2, sunt complete, exacte și actualizate.

([4]) Acest lucru nu aduce atingere delegării de competențe de la membrul național către adjunctul său, către alți membri ai personalului de la biroul național sau către personalul autorizat al Eurojust.

ANEXA II

STANDARDE PROCEDURALE DIGITALE

Articolul 3 punctul 9 din Regulamentul (UE) 2022/850 definește standardele procedurale digitale ca fiind specificațiile tehnice pentru modelele de procese operaționale și pentru schemele de date, care stabilesc structura electronică a datelor transmise prin intermediul sistemului e-CODEX.

Prezenta anexă stabilește specificațiile tehnice pentru modelele de procese operaționale și specificațiile tehnice ale schemelor de date.

1. **Specificații tehnice pentru modelele de procese operaționale în temeiul Regulamentului (UE) 2018/1727**

Specificațiile tehnice pentru modelele de procese operaționale sunt stabilite la punctele 1.1-1.5. Acestea definesc aspectele-cheie necesare pentru permiterea comunicării electronice în sensul Regulamentului (UE) 2018/1727 prin intermediul sistemului informatic descentralizat.

Sistemul informatic descentralizat permite schimbul de informații numai între autoritățile naționale competente ale unui stat membru și membrul național din statul membru respectiv.

1.1. *Schimbul de informații referitor la Registrul judiciar european de combatere a terorismului (CTR), articolul 21a din Regulamentul (UE) 2018/1727*

1.1.1. Model de transmitere a datelor CTR:

Autoritatea națională competentă transmite membrului național date privind procedurile în materie de terorism pentru CTR.

1.1.2. Model de primire a datelor CTR:

Membrul național primește datele CTR.

1.1.3. Model de solicitare a consimțământului:

Membrul național solicită consimțământul autorității sale naționale competente.

1.1.4. Model de primire a solicitării consimțământului:

Autoritatea națională competentă primește solicitarea consimțământului.

1.1.5. Model de transmitere a unui răspuns la solicitarea consimțământului:

Autoritatea națională competentă transmite un răspuns la solicitarea consimțământului.

1.1.6. Model de primire a unui răspuns la solicitarea consimțământului:

Membrul național primește răspunsul la solicitarea consimțământului.

1.1.7. Model de informare cu privire la legătură:

Membrul național informează autoritatea națională competentă cu privire la legătura cu un alt caz.

1.1.8. Model de actualizare a datelor CTR:

Autoritatea națională competentă transmite membrului său național datele care trebuie actualizate sau șterse.

1.1.9. Model de primire a datelor CTR actualizate:

Membrul național primește datele CTR care trebuie actualizate sau șterse.

1.2. *Schimbul de informații privind formele grave de criminalitate, articolul 21 din Regulamentul (UE) 2018/1727*

1.2.1. Model de transmitere a datelor privind formele grave de criminalitate transfrontalieră:

Autoritatea națională competentă transmite Eurojust date privind formele grave de criminalitate transfrontalieră.

1.2.2. Model de primire a datelor privind formele grave de criminalitate transfrontalieră:

Membrul național primește datele privind formele grave de criminalitate transfrontalieră.

1.2.3. Model de solicitare a consimțământului:

Membrul național solicită consimțământul autorității sale naționale competente.

1.2.4. Model de primire a solicitării consimțământului:

Autoritatea națională competentă primește solicitarea consimțământului.

1.2.5. Model de transmitere a unui răspuns la solicitarea consimțământului:

Autoritatea națională competentă transmite un răspuns la solicitarea consimțământului.

1.2.6. Model de primire a unui răspuns la solicitarea consimțământului:

Membrul național primește răspunsul la solicitarea consimțământului.

1.2.7. Model de informare cu privire la legătură:

Membrul național informează autoritatea națională competentă cu privire la legătura cu un alt caz.

1.2.8. Model de actualizare a datelor privind formele grave de criminalitate transfrontalieră:

Autoritatea națională competentă transmite membrului său național datele care trebuie actualizate sau șterse.

1.2.9. Model de primire a datelor privind formele grave de criminalitate transfrontalieră actualizate:

Membrul național primește datele privind formele grave de criminalitate transfrontalieră care trebuie actualizate sau șterse.

1.3. *Schimbul de informații generale*

1.3.1. Model de transmitere de informații:

Membrul național transmite informații autorității naționale competente sau viceversa.

1.3.2. Model de primire de informații:

Autoritatea națională competentă sau membrul național primește informațiile.

1.3.3. Model de răspuns la informații:

Autoritatea națională competentă răspunde la informațiile primite de la membrul național sau viceversa.

1.3.4. Model de primire a răspunsului:

Membrul național primește răspunsul din partea autorității naționale competente.

1.3.5. Model de transmitere de informații:

Autoritatea națională competentă transmite informații membrului național.

1.3.6. Model de primire de informații:

Membrul național primește informațiile.

1.3.7. Model de răspuns la informații:

Membrul național răspunde la informațiile primite de la autoritatea națională competentă.

1.3.8. Model de primire a răspunsului:

Autoritatea națională competentă primește răspunsul din partea membrului național.

1.4. *Rolul de facilitare și de sprijinire, articolul 8 alineatul (1) din Regulamentul (UE) 2018/1727*

Notă: În cazul în care modelele de facilitare și de sprijin prezentate la punctul 1.5 implică schimbul de formate statutare stabilite prin acte juridice ale Uniunii în domeniul cooperării judiciare în materie penală, modelele utilizează, dacă sunt disponibile, reprezentările de date structurate relevante și schemele XML elaborate pentru actele respective, de exemplu cele stabilite în scopul punerii în aplicare a Regulamentului (UE) 2023/2844 sau a altor instrumente relevante.

1.5. *Model de cerere de facilitare sau de sprijin*

1.5.1. Model de transmitere a cererii de facilitare sau de sprijin:

Autoritatea națională competentă transmite o cerere de facilitare sau de sprijin membrului său național respectiv.

1.5.2. Model de primire a cererii de facilitare sau de sprijin:

Membrul național primește cererea de facilitare sau de sprijin și o transmite membrului național al statului membru solicitat în afara JUDEX.

1.5.3. Model de transmitere a cererii de facilitare sau de sprijin către autoritatea națională competentă:

Membrul național al statului membru solicitat transmite cererea autorității sale naționale competente respective.

1.5.4. Model de primire a cererii de facilitare sau de sprijin:

Autoritatea națională competentă primește cererea de facilitare sau de sprijin.

1.5.5. Model de transmitere a răspunsului la cererea de facilitare sau de sprijin:

Autoritatea națională competentă transmite membrului național al statului membru solicitat un răspuns la cerere sau informații cu privire la aceasta.

1.5.6. Model de primire a unui răspuns la cererea de facilitare sau de sprijin:

Membrul național primește răspunsul sau informațiile privind cererea de facilitare sau de sprijin din partea autorității naționale competente și o comunică membrului național al statului membru solicitant în afara JUDEX.

1.5.7. Model de răspuns la cererea de facilitare sau de sprijin:

Membrul național al statului membru solicitant răspunde sau comunică informațiile referitoare la cererea de facilitare sau de sprijin din partea autorității naționale competente.

1.5.8. Model de primire a răspunsului:

Autoritatea națională competentă primește răspunsul sau informațiile privind cererea de facilitare sau de sprijin.

2. **Specificații tehnice pentru schemele de date**

Specificațiile tehnice care vor servi drept bază pentru elaborarea definițiilor schemelor XML (XSD) pentru digitalizarea Regulamentului (UE) 2018/1727 sunt stabilite la punctele 2.1 și 2.2 din prezenta anexă. Aceste specificații definesc componentele-cheie și orice alte informații pentru a furniza o descriere cuprinzătoare a elaborării acestor scheme.

Descrierea se dorește a fi generică, permițând ca XSD-urile elaborate să fie modificate și extinse fără a necesita modificări semnificative ale prezentelor specificații.

Specificațiile se aplică formatului statutar al schemelor anexate la Regulamentul (UE) 2018/1727, mesajelor predefinite sau mesajelor cu text liber utilizate în schimburile efectuate în temeiul regulamentului respectiv.

2.1. *Considerații generale*

Pentru toate schemele care trebuie furnizate, se aplică următoarele dispoziții:

2.1.1. Gestionarea versiunilor

Se include un atribut al versiunii care facilitează gestionarea versiunilor schemei și permite actualizarea schemei în iterații viitoare, în funcție de cerințele operaționale. Atributul versiunii indică dacă noua versiune este compatibilă cu versiunile anterioare atunci când se introduc noi caracteristici sau îmbunătățiri.

2.1.2. Declarația privind schema și metadatele

— După caz, schema utilizează standardele sau vocabularele relevante, impuse de e-CODEX pentru a asigura interoperabilitatea, care sunt necesare pentru validarea corespunzătoare a elementelor și tipurilor definite în cadrul acestei scheme. Acestea pot include:

  — vocabularul de bază al UE în domeniul e-justiției;

  — tipurile de date necalificate;

  — o listă de coduri pentru codurile lingvistice ale Uniunii Europene.

— De asemenea, după caz, schema poate include standarde ETSI relevante pentru a utiliza definițiile acestora.

2.1.3. Adnotări și documentație

— **Adnotări**: Fiecare element al schemei trebuie, de regulă, să fie însoțit de adnotări. Adnotările oferă informații lizibile pentru om cu privire la element, definind adesea scopul sau utilizarea acestuia într-un mod clar și concis.

2.1.4. Utilizare și adaptabilitate

Schema respectă normele prevăzute la literele (a)-(d):

(a) **Structură modulară**: fiecare secțiune este proiectată cu funcționalitate specifică și poate fi reutilizată sau adaptată în mod independent. Astfel, schema va fi ușor de adaptat pentru diferite cazuri de utilizare.

(b) **Extensibilitate**: schema este concepută astfel încât să sprijine includerea de noi elemente sau atribute în cazul în care vor fi necesare informații suplimentare în viitor. Acest lucru se realizează prin utilizarea de elemente și secvențe opționale care pot fi extinse fără a afecta implementările existente.

(c) **Structură adaptabilă**: schema este concepută astfel încât să permită adăugarea sau modificarea elementelor sau a tipurilor de date, după caz. Structura schemei trebuie să țină seama de modificările cerințelor, fără a fi necesare reconfigurări majore.

(d) **Elemente opționale**: elementele din cadrul unei scheme pot fi marcate ca opționale, adică pot fi incluse sau omise în funcție de circumstanțe specifice.

Schema este concepută pentru a sprijini colectarea de date structurate pentru cereri specifice.

2.1.5. Modificări

Structura schemei se caracterizează prin flexibilitate, modularitate și ușurința adaptării. Tipurile complexe și elementele opționale sunt încorporate în proiectare, astfel încât să permită gestionarea unor scenarii diverse, rămânând în același timp ușor de modificat și de extins.

2.2. *Schimbul de date structurate*

Datele structurate menționate la punctele 2.2.1 și 2.2.2 se furnizează în conformitate cu articolul 22a alineatul (3) din Regulamentul (UE) 2018/1727. Schema permite, de asemenea, indicarea seturilor de date care urmează să fie șterse în actualizările viitoare.

2.2.1. Date din Registrul judiciar european de combatere a terorismului

Următoarele specificații tehnice pentru schema de date stabilesc un cadru structurat pentru crearea schemei în format XML.

(a) Secțiunea de nivel superior

Această secțiune de nivel superior corespunde informațiilor prevăzute în anexa III la Regulamentul (UE) 2018/1727, informații pentru Registrul judiciar european de combatere a terorismului (CTR).

(b) Structura mesajului

Structura datelor CTR constă într-o secvență de elemente și include cel puțin:

(i) Informații pentru identificarea persoanelor fizice:

— numele (numele de familie);

— prenumele;

— orice pseudonime;

— data nașterii;

— locul nașterii (localitatea și țara);

— cetățenia sau cetățeniile;

— actul de identitate (tipul și numărul documentului);

— genul;

— locul de reședință.

(ii) Informații pentru identificarea persoanelor juridice:

— denumirea comercială;

— forma juridică;

— locul în care se află sediul social.

(iii) Informații atât pentru identificarea persoanelor fizice, cât și a persoanelor juridice:

— numerele de telefon;

— adresele de e-mail;

— detaliile privind conturile deținute la bănci sau la alte instituții financiare;

— stadiul procedurii.

(iv) Informații privind infracțiunea:

— informații privind persoanele juridice implicate în pregătirea sau comiterea unei infracțiuni de terorism;

— calificarea juridică a infracțiunii în temeiul dreptului intern;

— forma aplicabilă a infracțiunii grave din lista menționată în anexa I;

— orice afiliere la o grupare teroristă;

— tipul de terorism, cum ar fi jihadist, separatist, de stânga sau de dreapta;

— rezumat succint al cazului.

(v) Informații privind procedurile naționale:

— stadiul procedurilor respective;

— parchetul responsabil;

— numărul cazului;

— data inițierii procedurii judiciare oficiale;

— legăturile cu alte cazuri conexe.

(vi) Câmp pentru informații suplimentare (text liber).

(vii) Codul autorizării prealabile.

2.2.2. Date transmise în conformitate cu articolul 21 din Regulamentul (UE) 2018/1727

(a) Articolul 21 alineatul (4) din Regulamentul (UE) 2018/1727 privind constituirea de echipe comune de anchetă (JIT)

(i) Secțiunea de nivel superior
Această secțiune de nivel superior corespunde informațiilor prevăzute la articolul 21 alineatul (4) din Regulamentul (UE) 2018/1727, informații privind constituirea echipelor comune de anchetă.

(ii) Structura mesajului
Structura datelor constă într-o secvență de elemente și include cel puțin:

— Autoritatea judiciară națională responsabilă cu procedura penală;

— Numărul național de referință al procedurii penale;

— Stadiul procedurii penale;

— Infracțiuni anchetate;

— Alte țări implicate în caz;

— Caz deja sprijinit de Eurojust?

— În caz afirmativ, numărul de identificare al cazului Eurojust?

— În caz negativ, este vorba despre o cerere de sprijin?

— Caz sprijinit de Europol?

— În caz afirmativ, grupul operativ („OTF”) și/sau aplicație de rețea pentru schimbul securizat de informații („SIENA”)?

— Acord JIT:

— Țări implicate;

— Părțile JIT (autoritățile naționale responsabile de anchete);

— Numărul național de referință al procedurilor penale care fac obiectul JIT;

— Data semnării;

— Durată;

— Infracțiuni anchetate;

— Rezumat succint al cazului;

— Principalii suspecți în cadrul procedurilor penale care fac obiectul JIT (numele, prenumele, data și locul nașterii și, eventual, alte categorii de date relevante și necesare în conformitate cu anexa II);

— Rezultatele activității echipelor comune de anchetă:

— Dificultăți/întârzieri privind:

— constituirea JIT;

— solicitarea/schimbul de probe în cadrul JIT;

— convenirea asupra/punerea în aplicare a unei strategii comune în materie de urmărire penală;

— Admisibilitatea/inadmisibilitatea/evaluarea probelor JIT în cadrul procedurilor naționale;

— Rezultatul procedurilor judiciare (urmăriri penale reușite/nereușite și condamnări/achitări).

(iii) Codul autorizării prealabile

(b) Articolul 21 alineatul (5) din Regulamentul (UE) 2018/1727, cazuri grave și complexe

(i) Secțiunea de nivel superior

Această secțiune de nivel superior corespunde informațiilor prevăzute la articolul 21 alineatul (5) din Regulamentul Eurojust, și anume cazurilor grave și complexe.

(ii) Structura mesajului

Structura datelor constă într-o secvență de elemente și include cel puțin:

— Autoritatea judiciară națională responsabilă cu procedura penală;

— Numărul național de referință al procedurii penale;

— Stadiul procedurii penale;

— Infracțiuni anchetate;

— Alte țări implicate în caz;

— Caz deja sprijinit de Eurojust?

— În caz afirmativ, numărul de identificare al cazului Eurojust?

— În caz negativ, este vorba despre o cerere de sprijin?

— Caz sprijinit de Europol?

— În caz afirmativ, grupul operativ și/sau SIENA?

— Forma aplicabilă de infracțiune gravă;

— Implicarea unei rețele de criminalitate organizată

— De tip mafiot;

— Rețea transnațională de criminalitate organizată.

— Repercusiuni la nivelul UE;

— Principalii suspecți în cadrul procedurilor penale (numele, prenumele, data și locul nașterii și, eventual, alte categorii de date relevante și necesare în conformitate cu anexa II);

— Rezumat succint al cazului;

— Alte țări implicate;

— Țări cu care cooperarea a fost deja inițiată;

— Autorități competente implicate în altă țară;

— Instrumentele de cooperare judiciară utilizate;

— Numărul de cereri transmise/primite;

— Existența unor investigații conexe;

— Țări cu care urmează să fie activată cooperarea/țări care ar putea fi afectate

— Tipul de cooperare necesară (cum ar fi extrădare, strângere de probe, alte forme de cooperare).

— Existența unor investigații conexe.

(iii) Codul autorizării prealabile

(c) Articolul 21 alineatul (6) litera (a) din Regulamentul (UE) 2018/1727, conflicte de jurisdicție

(i) Secțiunea de nivel superior

Această secțiune de nivel superior corespunde informațiilor prevăzute la articolul 21 alineatul (6) litera (a) din Regulamentul (UE) 2018/1727, și anume conflictelor de jurisdicție.

(ii) Structura mesajului

Structura datelor constă într-o secvență de elemente și include cel puțin:

— Autoritatea judiciară națională responsabilă cu procedura penală;

— Numărul național de referință al procedurii penale;

— Stadiul procedurilor penale (de exemplu, cercetare, trimitere în judecată, judecată);

— Infracțiuni anchetate;

— Alte țări implicate în caz;

— Caz deja sprijinit de Eurojust?

— În caz afirmativ, numărul de identificare al cazului Eurojust?

— În caz negativ, este vorba despre o cerere de sprijin?

— Caz sprijinit de Europol?

— În caz afirmativ, grupul operativ și/sau SIENA?

— Alte țări implicate;

— Autoritățile naționale competente din cealaltă țară, dacă sunt cunoscute;

— Numărul național de referință al procedurilor penale din altă țară;

— Stadiul procedurilor în altă țară, dacă este cunoscut.

— Conflict pozitiv sau negativ;

— Conflict real sau potențial;

— Activități de coordonare deja întreprinse [de exemplu, consultări în temeiul Deciziei-cadru 2009/948/JAI a Consiliului ([1])]

— Rezumat succint al cazului;

— Principalii suspecți comuni (numele, prenumele, data și locul nașterii și, eventual, alte categorii relevante și necesare de date în conformitate cu anexa II).

(iii) Codul autorizării prealabile

(d) Articolul 21 alineatul (6) litera (b), livrări supravegheate

(i) Secțiunea de nivel superior
Această secțiune de nivel superior corespunde informațiilor prevăzute la articolul 21 alineatul (6) litera (b) din Regulamentul (UE) 2018/1727: livrări supravegheate.

(ii) Structura mesajului
Structura datelor constă într-o secvență de elemente și include cel puțin:

— Autoritatea judiciară națională responsabilă cu procedura penală;

— Numărul național de referință al procedurii penale;

— Stadiul procedurilor penale (de exemplu, cercetare, trimitere în judecată, judecată);

— Infracțiuni anchetate;

— Alte țări implicate în caz;

— Caz deja sprijinit de Eurojust?

— În caz afirmativ, numărul de identificare al cazului Eurojust?

— În caz negativ, este vorba despre o cerere de sprijin?

— Caz sprijinit de Europol?

— În caz afirmativ, grupul operativ și/sau SIENA?

— Alte țări implicate;

— Țara de origine/tranzit/destinație;

— Autoritățile naționale competente din alte țări;

— Existența unor anchete conexe în alte țări.

([1]) Decizia-cadru 2009/948/JAI a Consiliului din 30 noiembrie 2009 privind prevenirea și soluționarea conflictelor referitoare la exercitarea competenței în cadrul procedurilor penale (JO L 328, 15.12.2009, p. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Tipul de mărfuri livrate (de exemplu, droguri și tip/bani/arme/țigări/altele);

— Stadiul livrării supravegheate (de exemplu, planificată, în curs, finalizată);

— Rezultatul livrării supravegheate, dacă a fost deja efectuată;

— Instrument de cooperare judiciară utilizat;

— Principalii suspecți comuni (numele, prenumele, data și locul nașterii și, eventual, alte categorii relevante și necesare de date în conformitate cu anexa II).

(iii) Codul autorizării prealabile

(e) Articolul 21 alineatul (6) litera (c) din Regulamentul (UE) 2018/1727, dificultăți repetate legate de instrumentele de cooperare judiciară

(i) Secțiunea de nivel superior

Această secțiune de nivel superior corespunde informațiilor prevăzute la articolul 21 alineatul (6) litera (c) din Regulamentul (UE) 2018/1727: dificultăți repetate legate de instrumentele de cooperare judiciară.

(ii) Structura mesajului

Structura datelor constă într-o secvență de elemente și include cel puțin:

— Autoritatea judiciară națională responsabilă cu procedura penală;

— Numărul național de referință al procedurii penale;

— Stadiul procedurilor penale (de exemplu, cercetare, trimitere în judecată, judecată);

— Infracțiuni anchetate;

— Alte țări implicate în caz;

— Caz deja sprijinit de Eurojust?

— În caz afirmativ, numărul de identificare al cazului Eurojust?

— În caz negativ, este vorba despre o cerere de sprijin?

— Caz sprijinit de Europol?

— În caz afirmativ, grupul operativ și/sau SIENA?

— Alte țări implicate;

— Autoritățile naționale competente, dacă sunt cunoscute;

— În calitate de autoritate emitentă sau executantă;

— Instrumentul de cooperare judiciară implicat (de exemplu, mandat european de arestare, ordinul european de anchetă, sechestrare și confiscare);

— Cerere specifică vizată (și anume măsura de investigare, tipul de sechestrare, mandat european de arestare pentru executarea pedepsei sau pentru urmărirea penală).

— Refuz sau dificultate repetată;

— În caz de refuz, care este motivul specific invocat?

— Scurtă descriere a chestiunii.

— Alte autorități naționale afectate de aceeași problemă, dacă este cazul.

(iii) Codul autorizării prealabile

2.3. *Codurile autorizărilor prealabile*

Atunci când fac schimb de date cu Eurojust prin intermediul JUDEX, autoritățile naționale competente indică, prin intermediul codurilor de autorizare prealabilă, gestionarea ulterioară, accesarea și transferul de date în urma identificării unei legături. Codurile de autorizare prealabilă indică dacă și în ce măsură informațiile referitoare la legătură pot fi partajate cu alte autorități naționale competente, alte agenții și organisme ale Uniunii, țări terțe sau organizații internaționale.

2.4. *Mesaje predefinite*

Mesajele predefinite sunt reprezentări ale schimburilor instituite prin Regulamentul (UE) 2018/1727, dar pentru care nu a fost prevăzut niciun format specific în actul juridic. Tipurile și numărul lor sunt determinate în cursul analizei operaționale și tehnice.

Definițiile schemelor XML (XSD) pentru mesajele predefinite trebuie concepute astfel încât să asigure coerența, structura și conformitatea cu nevoile operaționale.

Schemelor respective li se aplică următoarele dispoziții:

(a) secțiunea de nivel superior din această schemă se denumește în funcție de tipul specific de mesaj definit;

(b) câmpurile necesare pentru tipul specific de mesaj se adaugă și se definesc în cadrul acestei structuri, asigurându-se reprezentarea corespunzătoare a elementelor de date.

2.5. *Mesaje cu text liber*

Mesajele cu text liber sunt reprezentări ale schimburilor care permit un conținut nestructurat sau parțial structurat, permițând flexibilitatea și respectând în același timp cerințele de reglementare și operaționale. XSD pentru mesajele cu text liber trebuie concepute astfel încât să asigure coerența și formatarea corespunzătoare.

Schemelor respective li se aplică următoarele dispoziții:

(a) secțiunea de nivel superior din schemă se denumește în funcție de tipul specific de mesaj cu text liber definit;

(b) schema definește structura necesară pentru mesajul cu text liber, permițând în același timp ordonarea adecvată a elementelor, după caz;

(c) câmpurile necesare pentru tipul specific de mesaj cu text liber se adaugă și se definesc în cadrul acestei structuri, asigurându-se reprezentarea corespunzătoare a elementului de date.

ANEXA III

SPECIFICAȚII TEHNICE PRIVIND AMPRENTELE DIGITALE ȘI FOTOGRAFIILE

Mesajele transmise prin intermediul sistemului informatic descentralizat pot fi însoțite de documentele atașate, inclusiv de fișiere de la Institutul Național pentru Standarde și Tehnologie (*National Institute of Standards and Technology* – NIST) care conțin amprente digitale și fotografii, în conformitate cu specificațiile tehnice prevăzute la punctele 1 și 2.

1. **Amprente digitale**

Amprentele digitale care pot fi partajate cu Eurojust în scopul identificării fiabile a persoanelor care fac obiectul procedurilor penale legate de infracțiuni de terorism trebuie să îndeplinească următoarele condiții:

(a) amprentele digitale sunt furnizate într-un fișier care conține imagini digitale ale amprentelor digitale (fișierul NIST cu amprente digitale) și sunt transmise în conformitate cu standardul ANSI/NIST-ITL 1-2011: Update 2015 (sau o versiune mai recentă);

(b) fișierul NIST cu amprente digitale conține până la zece amprente digitale individuale: rulate, plane sau ambele;

(c) toate amprentele digitale sunt etichetate;

(d) amprentele digitale sunt captate prin scanări în direct sau cu cerneală pe hârtie, cu condiția ca amprentele digitale prelevate cu cerneală pe hârtie să fi fost scanate la rezoluția prevăzută și la același nivel de calitate;

(e) fișierul NIST cu amprente digitale permite includerea de informații suplimentare, cum ar fi condițiile de înregistrare a amprentelor digitale și metoda utilizată pentru obținerea imaginilor dactiloscopice individuale;

(f) amprentele digitale au o rezoluție nominală de 500 sau de 1 000 ppi ([1]) (cu o abatere acceptabilă de +/– 10 ppi) cu 256 de niveluri de gri;

(g) algoritmul de compresie a amprentelor digitale care trebuie utilizat respectă recomandările Institutului Național pentru Standarde și Tehnologie („NIST”). Datele dactiloscopice cu o rezoluție de 500 ppi sunt comprimate utilizând algoritmul WSQ (ISO/IEC 19794-5:2005). Pentru comprimarea datelor dactiloscopice cu o rezoluție de 1 000 ppi se utilizează standardul de compresie a imaginilor (ISO/IEC 15444-1) și sistemul de codificare JPEG 2000. Rata de compresie țintă este 15:1.

2. **Fotografii**

Fotografiile care pot fi partajate cu Eurojust în scopul identificării fiabile a persoanelor care fac obiectul procedurilor penale legate de infracțiuni de terorism trebuie să îndeplinească următoarele condiții:

(a) o singură imagine facială este furnizată într-un fișier de tip fotografie (fișierul fotografie NIST) și este transmisă în conformitate cu standardul ANSI/NIST-ITL 1-2011: Update 2015 sau cu orice versiune mai recentă disponibilă;

(b) fotografiile sunt fie în tonuri de gri, fie color, fie în infraroșu apropiat;

(c) calitatea fotografiilor se bazează pe cerințele privind imaginea din ISO/IEC 19794-5:2011, Tipul de imagine frontală, sau orice versiune mai recentă disponibilă;

(d) fișierul fotografie NIST permite includerea de informații suplimentare, inclusiv data la care a fost realizată imaginea;

([1]) Pixeli pe inch.

(e) fotografiile, în modul portret, au o rezoluție minimă de 600 de pixeli pe 800 de pixeli și o rezoluție maximă de 1 200 de pixeli pe 1 600 de pixeli;

(f) fața ocupă un spațiu în cadrul fotografiei care asigură minimum 120 de pixeli între părțile centrale ale ochilor.

(g) algoritmul de compresie a fotografiilor utilizat respectă recomandările Institutului Național pentru Standarde și Tehnologie („NIST”). Fotografiile sunt comprimate o singură dată la o compresie a imaginii și cu sistemul de codificare JPG (ISO/IEC 10918) sau JPEG 2000 (ISO/IEC 15444), la un raport maxim permis de compresie a imaginii de 20:1.