Official Journal
of the European Union

EN
L series

2025/2447

5.12.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/2447

of 4 December 2025

laying down the rules for the application of Regulation (EU) 2018/1727 of the European Parliament and of the Council, as regards the technical specifications, measures and other requirements for the establishment and use of the decentralised IT system for secure processing and communication of information

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Agency for Criminal Justice Cooperation (Eurojust) and replacing and repealing Council Decision 2002/187/JHA ([1]), and in particular Article 22a(3) and Article 22b(1), points (a), (b), (c) and (d), thereof,

Whereas:

(1) Regulation (EU) 2018/1727 sets out the framework for Eurojust's new digital internal infrastructure and the establishment of a decentralised secure digital communication system between the competent national authorities of the Member States and Eurojust.

(2) The secure digital communication is to be carried out through the decentralised IT system. To establish the decentralised IT system, it is necessary to set out technical specifications defining the methods of communication and communication protocols, technical measures ensuring minimum information security standards and security and minimum availability objectives for the implementation of that system.

(3) In accordance with Article 22a(1)of Regulation (EU) 2018/1727, the decentralised IT system is to be comprised of IT systems of the Member States and Eurojust, and interoperable e-CODEX access points through which those IT systems are interconnected. The technical specifications and other requirements of the decentralised IT system set out in this Regulation should take that framework into account.

(4) The access points of the decentralised IT system should be based on authorised e-CODEX access points as defined in Article 3(3) of Regulation (EU) 2022/850 of the European Parliament and of the Council ([2]).

(5) The decentralised IT system is implemented within a larger e-CODEX-based decentralised IT system referred to as the Justice Digital Exchange System (JUDEX). Therefore, it is necessary to ensure an effective exchange of information concerning horizontal developments.

(6) In accordance with Article 22a(4) of Regulation (EU) 2018/1727, Member States and Eurojust may choose to use the reference implementation software developed by the Commission as their back-end system instead of a national IT system. In order to ensure interoperability, both national IT systems and the reference implementation software should be subject to the same technical specifications and requirements.

(7) Data relating to terrorist offences and serious organised crime should be transmitted in a structured manner to improve the quality and relevance of the information, as well as to ensure that the information can be more efficiently integrated into Eurojust's case management system and better cross-checked against information already stored in that system. For fingerprint data and photographs, which may be transmitted to Eurojust for the purpose of identifying individuals subject to criminal proceedings related to terrorism offences, the format and technical standards for the transmission should be defined.

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

([2]) Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ L 150, 1.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust facilitates and supports the issuance and execution of judicial cooperation requests, including requests and decisions based on instruments that give effect to the principle of mutual recognition. National competent authorities should be able to seek assistance and coordination from Eurojust through the decentralised IT system.

(9) In order to ensure efficiency and consistency, it is important that the technical specifications to be established under Regulation (EU) 2018/1727 are compatible with the technical specifications established under Regulations (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) and (EU) 2024/3011 ([5]) of the European Parliament and of the Council as well as with future digitalisation measures relevant to Eurojust's mandate to support national competent authorities.

(10) Any other communication between Eurojust and the competent national authorities, such as communication of information on the results of the processing of information, including the existence of links with cases already stored in the case management system in accordance with Article 22 of Regulation (EU) 2018/1727 when Eurojust is acting on own initiative, or of information transmitted to Eurojust for the purpose of preserving, analysing and storing evidence related to genocide, crimes against humanity, war crimes and related criminal offences in accordance with Article 4(1), point (j) of that Regulation, should also be enabled through the decentralised IT system.

(11) To ensure that this Regulation takes into account the operational needs of Eurojust, Eurojust has been consulted in accordance with Article 22a(3) of Regulation (EU) 2018/1727.

(12) In accordance with Article 4 of Protocol No 21 on the position of the United Kingdom and Ireland in respect to area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Ireland has notified, by letter of 9 September 2019, its wish to accept and be bound by Regulation (EU) 2018/1727. Commission Decision (EU) 2019/2006 ([6]) confirmed such participation. Regulation (EU) 2023/2131 of the European Parliament and of the Council ([7]) amended Regulation (EU) 2018/1727 to enable the establishment of secure digital communication channels between Eurojust and the competent national authorities and provides the legal basis for this Regulation. In circumstances where Ireland did not notify its wish to take part in the adoption and application of Regulation (EU) 2023/2131 and has not notified its wish to accept and be bound by that Regulation, Ireland, in accordance with Articles 1, 2 and Article 4a(1) of Protocol No 21, is not bound by Regulation (EU) 2023/2131 or subject to its application. Ireland is therefore not taking part in the adoption of this Regulation.

(13) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark did not take part in the adoption of Regulation (EU) 2018/1727. Denmark is therefore not bound by this Regulation or subject to its application.

([3]) Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation (OJ L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Regulation (EU) 2024/3011 of the European Parliament and of the Council of 27 November 2024 on the transfer of proceedings in criminal matters (OJ L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Commission Decision (EU) 2019/2006 of 29 November 2019 on the participation of Ireland in Regulation (EU) 2018/1727 of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) (OJ L 310, 2.12.2019, p. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Regulation (EU) 2023/2131 of the European Parliament and of the Council of 4 October 2023 amending Regulation (EU) 2018/1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA, as regards digital information exchange in terrorism cases (OJ L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([8]) and delivered an opinion on 21 October 2025.

(15) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 22c of Regulation (EU) 2018/1727,

HAS ADOPTED THIS REGULATION:

Article 1

Technical specifications of the decentralised IT system

The technical specifications, measures and objectives of the decentralised IT system referred to in Article 22b(1), point (a), (b), (c) and (d), of Regulation (EU) 2018/1727 shall be as set out in Annex I to this Regulation.

Article 2

Digital procedural standards

The digital procedural standards applicable to the electronic communication through the decentralised IT system referred to in Article 22a(3) of Regulation (EU) 2018/1727 shall be as set out in Annex II to this Regulation.

Article 3

Technical specifications for the transmission of fingerprints and photographs

The technical specifications and the format for the transmission of fingerprints and photographs ~~as~~ referred to in Article 22a(3) of Regulation (EU) 2018/1727 shall be as set out in Annex III to this Regulation.

Article 4

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels, 4 December 2025.

For the Commission
The President
Ursula VON DER LEYEN

([8]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANNEX I

TECHNICAL SPECIFICATIONS, MEASURES AND OBJECTIVES OF THE DECENTRALISED IT SYSTEM

1. **Introduction and scope**

This Annex sets out the technical specifications, measures and objectives of the decentralised IT system for the exchange of information under Regulation (EU) 2018/1727.

The decentralised nature of the IT system enables data to be directly and securely exchanged between competent national authorities and Eurojust.

2. **Definitions**

For the purpose of this Annex, the following definitions apply:

2.1. 'Hypertext Transfer Protocol Secure' or 'HTTPS' means encrypted communication and secure connection channels;

2.2. 'non-repudiation of origin' means the measures providing the proof of the integrity and proof of origin of the data through methods such as digital certification, public key infrastructure and electronic signatures and electronic seals;

2.3. 'non-repudiation of receipt' means the measures providing the proof of the receipt of the data to the originator by the intended recipient of the data through methods such as digital certification, public key infrastructure, electronic signatures and electronic seals;

2.4. 'SOAP' (Simple Object Access Protocol) means, as per the standards of the World Wide Web Consortium, a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks;

2.5. 'REST' (Representational State Transfer) means an architectural style for designing networked applications, relying on a stateless, client-server communication model, using standard methods to perform operations on resources which are typically represented in structured formats;

2.6. 'web service' means a software system designed to support interoperable machine-to-machine interaction over a network, and which has an interface described in a machine-processable format;

2.7. 'data exchange' means the exchange of messages and documents through the decentralised IT system;

2.8. 'e-CODEX' means the e-CODEX system as defined in Article 3(1) of Regulation (EU) 2022/850;

2.9. 'EU e-Justice Core Vocabularies' means the EU e-Justice Core Vocabularies as defined in point 4 of the Annex to Regulation (EU) 2022/850;

2.10. 'ebMS' refers to the ebXML Message Service, a messaging protocol developed under the OASIS framework that enables secure, reliable, and interoperable exchange of electronic business documents using SOAP. It supports business-to-business integration across diverse systems;

2.11. 'AS4' stands for Applicability Statement 4, an OASIS standard that profiles ebMS 3.0; whereas it simplifies secure and interoperable business-to-business messaging by using open standards such as SOAP and WS-Security;

2.12. ‘Recovery Time Objective’ means the maximum acceptable time to restore service after an incident;

2.13. ‘Recovery Point Objective’ means the maximum acceptable amount of data loss in case of failure.

3. **Methods of communication by electronic means**

3.1. The decentralised IT system shall use service-based methods of communication, such as web services or other reusable components and software solutions for the purpose of exchanging messages and documents.

3.2. Specifically, the decentralised IT system shall involve communication through e-CODEX access points, as set out in Article 5(2) of Regulation (EU) 2022/850. Therefore, to ensure effective and interoperable cross-border data exchange, the decentralised IT system shall support communication via the e-CODEX system.

4. **Communication protocols**

4.1. The decentralised IT system shall use secure internet protocols for:

(a) communication within the decentralised IT system between competent authorities and Eurojust;

(b) communication with the Competent authority/ Court database as referred to in point 7.1.

4.2. For the definition and the transmission of structured data and metadata, the components of the decentralised IT system shall be based on comprehensive and broadly accepted industry standards and protocols, such as SOAP and REST.

4.3. For the Transport and Messaging Protocols, the decentralised IT system shall be based on secure standard-based protocols such as:

(a) AS4 Profile for cross-border data exchange, ensuring secure, reliable messaging with encryption and non-repudiation;

(b) HTTPS/RESTful APIs for communication supporting JSON and XML formats;

(c) SOAP for high-reliability interactions, incorporating WS-Security for authentication and encryption.

4.4. For the purpose of seamless and interoperable data exchange, the communication protocols used by the decentralised IT system shall comply with relevant interoperability standards.

4.5. Where applicable, the XML schemas shall make use of relevant standards or vocabularies, which are necessary for the proper validation of the elements and types defined within the schema. Those standards or vocabularies may include:

(a) EU e-Justice Core Vocabulary;

(b) Unqualified Data Types;

(c) A code list for the European Union language codes.

4.6. For the security and authentication protocols, the decentralised IT system shall be based on standards-based protocols such as:

(a) TLS (Transport Layer Security) for encrypted and authenticated communication over networks, supporting mutual authentication via X.509 digital certificates;

(b) OAuth / OpenID Connect (OIDC) for secure authentication and authorisation;

(c) PKI (public key infrastructure) and digital signatures for secure key exchange and message integrity verification, using digital certificates (X.509) issued by trusted Certification Authorities.

5. **Information security objectives and relevant technical measures**

5.1. For the exchange of information via the decentralised IT system, the technical measures for ensuring minimum information technology security standards shall include the following:

(a) measures to ensure confidentiality of information, including by using secure channels of communication;

(b) measures to ensure the integrity of data at rest and in transit;

(c) measures to ensure the non-repudiation of origin of the sender of information within the decentralised IT system and the non-repudiation of receipt of information;

(d) measures to ensure logging of security events in line with recognised international recommendations for information technology security standards ([1]);

(e) measures to ensure user authentication and authorisation, and measures to verify the identity of systems connected to the decentralised IT system.

5.2. The components of the decentralised IT system shall ensure secure communication and data transmission, by using encryption, public key infrastructure with digital certificates for authentication and secure key exchange, and secure messaging protocols such as AS4 (ebMS), RESTful APIs and SOAP to maintain message confidentiality and integrity.

5.3. Where TLS is employed in the context of the decentralised IT system, the latest stable version of the protocol shall be used, or, failing that, a version without known security vulnerabilities. Only key lengths that ensure an adequate level of cryptographic security shall be permitted, and cipher suites known to be insecure or deprecated shall not be used.

5.4. To the extent possible, PKI digital certificates used for the purposes of operation of the decentralised IT system shall be issued by Certification Authorities recognised as Qualified Trust Service Providers in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council ([2]). Measures shall be implemented to ensure that such certificates are used solely for their intended purposes, at the required level of trust, and in compliance with the applicable requirements of Regulation (EU) No 910/2014.

5.5. The components of the decentralised IT system shall be developed in accordance with the principle of data protection by design and by default, and appropriate administrative, organisational and technical measures shall be implemented to ensure a high level of cybersecurity.

5.6. The Commission shall design, develop and maintain the reference implementation software in compliance with the data protection requirements and principles laid down in Regulation (EU) 2018/1725. The reference implementation software provided by the Commission shall allow Member States to comply with their obligations in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council ([3]) and Directive (EU) 2016/680, as applicable.

([1]) Without prejudice to logging for security purposes, the logging mechanisms employed by the components of the decentralised IT system shall, as appropriate, allow to ensure compliance with the requirements set out in Article 88 of Regulation (EU) 2018/1725 and, where applicable, Article 25 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Member States which use a national back-end system different than the reference implementation software shall implement the necessary measures to ensure that their national back-end system complies with the requirements of Regulation (EU) 2016/679 and Directive (EU) 2016/680, as applicable.

5.8. Eurojust shall implement the necessary measures to ensure that its back-end system, or an instance of the reference implementation software it deploys, complies with the requirements of Regulations (EU) 2018/1725 and (EU) 2018/1727.

5.9. Member States and Eurojust shall establish robust mechanisms for threat detection and incident response to ensure timely identification, mitigation, and recovery from security incidents, in accordance with their relevant policies, for the IT systems under their responsibility that form part of the decentralised IT system.

6. **Minimum availability objectives**

6.1. Eurojust and the Member States shall ensure 24 hours, 7 days a week availability of the components of the decentralised IT system under their responsibility, with a target technical availability rate of at least 98 % on an annual basis, excluding scheduled maintenance.

6.2. The Commission shall ensure 24 hours, 7 days a week availability of the Court database, with a target technical availability rate of more than 99 % on an annual basis, excluding scheduled maintenance.

6.3. To the extent possible, during working days, maintenance operations shall be planned between 20:00h and 7:00h CET.

6.4. Member States shall notify the Commission, Eurojust and the other Member States of maintenance activities as follows:

(a) 5 working days in advance for maintenance operations that may cause an unavailability period of up to 4 hours;

(b) 10 working days in advance for maintenance operations that may cause an unavailability period between 4 and 12 hours;

(c) 30 working days in advance for maintenance operations that may cause an unavailability period of more than 12 hours.

6.5. Where Member States have fixed regular maintenance windows, they shall inform the Commission, Eurojust and the other Member States of the time and day(s) when such fixed regular windows are planned. By way of derogation from the obligations set out in sentence 1, if components of the decentralised IT system under the Member States' responsibility become unavailable during such a regular fixed window, Member States may choose not to notify the Commission on each occasion.

6.6. In the event of an unexpected technical failure of a component of the decentralised IT system under the Member States' responsibility, Member States shall inform the Commission and the other Member States of the failure without delay, and, if known, of the projected recovery timeframe.

6.7. Eurojust shall notify the Commission and the Member States of maintenance activities as follows:

(a) 5 working days in advance for maintenance operations that may cause an unavailability period of up to 4 hours;

(b) 10 working days in advance for maintenance operations that may cause an unavailability period between 4 and 12 hours;

(c) 30 working days in advance for maintenance operations that may cause an unavailability period of more than 12 hours.

6.8. Where Eurojust has fixed regular maintenance windows, Eurojust shall inform the Commission and the Member States of the time and day(s) when such fixed regular windows are planned. By way of derogation from the obligations set out in sentence 1, if components of the decentralised IT system under Eurojust's responsibility become unavailable during such a regular fixed window, Eurojust may choose not to notify the Commission on each occasion.

6.9. In the event of an unexpected technical failure of a component of the decentralised IT system under Eurojust's responsibility, Eurojust shall inform the Commission and the Member States of the failure without delay, and, if known, of the projected recovery timeframe.

6.10. In the event of an unexpected technical failure of the Competent authorities/Court database, the Commission shall inform Eurojust and the Member States without delay of the unavailability, and if known, of the projected recovery timeframe.

6.11. In the event of a service disruption, Member States and Eurojust shall ensure service is swiftly restored and data loss is minimal, in accordance with the Recovery Time Objective and Recovery Point Objective.

6.12. Member States and Eurojust shall implement appropriate measures to achieve the availability objectives outlined above and establish procedures for effectively responding to incidents.

7. **Competent authorities/Court database (CDB)**

7.1. Pursuant to Article 22a of Regulation (EU) 2018/1727, the decentralised IT system shall enable electronic communication between the competent national authorities and Eurojust. Considering the obligations to exchange information between competent national authorities and Eurojust under Articles 21, 21a and 22, but also the role of Eurojust in facilitating and supporting the issuing and execution of any request for mutual legal assistance or mutual recognition in accordance with Article 8(1) of Regulation (EU) 2018/1727, the competent authorities involved need to be clearly identifiable when using the decentralised IT system. Therefore, it is essential to establish an authoritative database of those authorities' information for the purposes of the decentralised IT system.

7.2. The CDB shall include the following information in a structured format:

(a) for the purposes of Article 8(1), 8(3), 8(4), Article 21, Article 21a and Article 22 of Regulation (EU) 2018/1727 information on the competent national authorities, including national correspondents as set out in Article 20 of that Regulation, as well as national members in accordance with Article 7 ([4]) of that Regulation;

(b) where relevant, information necessary to determine the geographical or substantive areas of the competent authorities' competence, or other relevant criteria necessary to establish their competence;

(c) information necessary for the correct technical message routing within the decentralised IT system.

7.3. The Commission shall be responsible for the development, maintenance, operation and support of the CDB;

7.4. The CDB shall enable Member States and Eurojust to update the information therein, and the competent national authorities and National Members participating in the decentralised IT system to programmatically access and retrieve information therein;

7.5. Access to the CDB shall be possible via a common communication protocol, regardless of whether the competent authorities connected to the decentralised IT system operate a national back-end system or a deployment of the reference implementation software;

7.6. Member States shall ensure that the information on their competent authorities in the CDB as set out in point 7.2 is complete, accurate and up to date.

([4]) This is without prejudice to the delegation of powers from the national member to their deputy, other staff at the national desk or authorised Eurojust staff.

ANNEX II

DIGITAL PROCEDURAL STANDARDS

Article 3(9) of Regulation (EU) 2022/850 defines digital procedural standards as the technical specifications for business process models and data schemas which set out the electronic structure of the data exchanged through the e-CODEX system.

This Annex sets out the technical specifications for business process models and the technical specifications of data schemas.

1. **Technical specifications for the business process models under Regulation (EU) 2018/1727**

The technical specifications for business process models are set out in points 1.1 to 1.5. They define the key aspects necessary for enabling electronic communication for the purposes of Regulation (EU) 2018/1727 through the decentralised IT system.

The decentralised IT system shall allow exchange of information only between the competent national authorities of a Member State and the national member from that Member State.

1.1. *Exchange of information related to the European Judicial Counter-Terrorism Register (CTR) Article 21a of Regulation (EU) 2018/1727*

1.1.1. Transmit CTR data model:

The competent national authority transmits data on terrorist proceedings for the CTR to the national member.

1.1.2. Receive CTR data model:

The national member receives the CTR data.

1.1.3. Request consent model:

The national member requests the consent of its competent national authority.

1.1.4. Receive consent request model:

The competent national authority receives the consent request.

1.1.5. Send reply to consent request model:

The competent national authority sends a reply to the consent request.

1.1.6. Receive reply to consent request model:

The national member receives the reply to the consent request.

1.1.7. Inform about link model:

The national member informs the competent national authority about the link with another case.

1.1.8. Update CTR data model:

The competent national authority transmits data which require updating or deletion to its respective national member.

1.1.9. Receive updated CTR data model:

The national member receives the CTR data which require updating or deletion.

1.2. *Exchange of information related to serious crime Article 21 of Regulation (EU) 2018/1727*

1.2.1. Transmit serious cross-border crime data model:

The national competent authority transmits data on serious cross-border crime to Eurojust.

1.2.2. Receive serious cross-border crime data model:

The national member receives the serious cross-border crime data.

1.2.3. Request consent model:

The national member requests the consent of its national competent authority.

1.2.4. Receive consent request model:

The competent national authority receives the consent request.

1.2.5. Send reply to consent request model:

The competent national authority sends a reply to the consent request.

1.2.6. Receive reply to consent request model:

The national member receives the reply to the consent request.

1.2.7. Inform about link model:

The national member informs the competent national authority about the link with another case.

1.2.8. Update serious cross-border crime data model:

The competent national authority transmits data which require updating or deletion to its respective national member.

1.2.9. Receive updated serious cross-border crime data model:

The national member receives the serious cross-border crime data which require updating or deletion.

1.3. *Exchange of general information*

1.3.1. Send information model:

The national member sends information to the competent national authority or vice versa.

1.3.2. Receive information model:

The competent national authority or national member receives the information.

1.3.3. Respond to information model:

The competent national authority responds to the information received from the national member or vice versa.

1.3.4. Receive response model:

The national member receives the response from the competent national authority.

1.3.5. Send information model:

The competent national authority sends information to the national member.

1.3.6. Receive information model:

The national member receives the information.

1.3.7. Respond to information model:

The national member responds to the information received from the competent national authority.

1.3.8. Receive response model:

The competent national authority receives the response from the national member.

1.4. *Facilitation and support role Article 8(1) of Regulation (EU) 2018/1727*

Note: Where the facilitation and support models outlined in point 1.5 involve the exchange of statutory forms established by Union legal acts in the area of judicial cooperation in criminal matters, the models shall, where available, use the relevant structured data representations and XML schemas developed for those acts, for example those established for the purposes of implementing Regulation (EU) 2023/2844 or other relevant instruments.

1.5. *Facilitation or support request model:*

1.5.1. Transmit facilitation or support request model:

The national competent authority transmits a facilitation request or support request to its respective national member.

1.5.2. Receive facilitation or support request model:

The national member receives the facilitation or support request and forwards it to the national member of the requested Member State outside of JUDEX.

1.5.3. Forward facilitation or support request to competent national authority model:

The national member of the requested Member State sends the request to its respective competent national authority.

1.5.4. Receive facilitation or support request model:

The competent national authority receives the facilitation or support request.

1.5.5. Send response to facilitation or support request model:

The competent national authority sends a response to or information concerning the request to the national member of the requested Member State.

1.5.6. Receive response to facilitation or support request model:

The national member receives the response to or information concerning the facilitation or support request from the competent national authority and shares it with the national member of the requesting Member State outside of JUDEX.

1.5.7. Respond to facilitation or support request model:

The national member of the requesting Member State responds to or shares the information concerning the facilitation or support request from the competent national authority.

1.5.8. Receive response model:

The competent national authority receives the response or information concerning the facilitation or support request.

2. Technical specifications for data schemas

The technical specifications that are to serve as a basis for developing XML Schema Definitions (XSDs) for the digitalisation of Regulation (EU) 2018/1727 are set out in points 2.1 and 2.2 of this Annex. These specifications define the key components, and any other information in order to provide a comprehensive description for the production of these schemas.

The description is intended to be generic allowing the produced XSDs to be modified and extended without requiring significant changes to these specifications.

The specifications shall apply to the statutory form of the schemas as annexed to the Regulation (EU) 2018/1727, any predefined messages, or any free text messages used in exchanges under that Regulation.

2.1. *General considerations*

For all schemas to be provided, the following provisions shall apply:

2.1.1. Versioning

A version attribute shall be included that facilitates schema versioning management and allows the schema to be updated in future iterations as per business requirements. The version attribute shall indicate whether the new version is backward compatible when introducing new features or refinements.

2.1.2. Schema declaration and metadata

— Where applicable, the schema shall make use of relevant standards or vocabularies, required by e-CODEX to provide interoperability, which are necessary for the proper validation of the elements and types defined within this schema. This may include:

  — EU e-Justice Core Vocabulary

  — Unqualified Data Types

  — A code list for European Union Language Codes

— Also, where applicable, the schema may incorporate relevant ETSI standards to make use of their definitions.

2.1.3. Annotations and Documentation

— **Annotations**: Each element in the schema shall typically be accompanied by annotations. The annotations provide human-readable information about the element, often defining its purpose or usage in a clear and concise manner.

2.1.4. Usage and adaptability

The schema shall follow the rules set out in point (a) to (d):

(a) **Modular structure**: each section shall be designed with specific functionality and may be reused or adapted independently. This shall make the schema easy to customise for different use cases.

(b) **Extensibility**: the schema shall be designed to support the inclusion of new elements or attributes if additional information is needed in the future. This shall be achieved by using optional elements and sequences that may be extended without breaking existing implementations.

(c) **Adaptable structure**: the schema shall be designed in a manner allowing for the addition or modification of elements or data types as necessary. The schema's structure shall accommodate changes in requirements without the need for major redesigns.

(d) **Optional elements**: elements within a schema may be marked as optional, that is to say they may be included or omitted based on specific circumstances.

The schema shall be designed to support the collection of structured data for specific requests.

2.1.5. Modifications

The schema design shall be characterised by flexibility, modularity and ease of adaptation. Complex types and optional elements shall be incorporated into the design in such a way that it may handle diverse scenarios while remaining easy to modify and extend.

2.2. *Exchange of structured data*

The structured data referred to in points 2.2.1 and 2.2.2 shall be provided in accordance with Article 22a(3) of Regulation (EU) 2018/1727. The schema shall also allow data sets to be indicated which are to be deleted in future updates.

2.2.1. European Judicial Counter-Terrorism Register data

The following technical specifications for the data schema establish a structured framework for creating the schema in XML format.

(a) Top-level section

This top-level section corresponds to the information set out in Annex III to Regulation (EU) 2018/1727 information for the European Judicial Counter-Terrorism Register (CTR).

(b) Structure of the message

The structure of the CTR data shall consist of a sequence of elements and include the following as a minimum:

(i) information for the identification of natural persons:

— surname (family name);

— first names (given names);

— any aliases;

— date of birth;

— place of birth (town and country);

— nationality or nationalities;

— identification document (type and document number);

— gender;

— place of residence;

(ii) information for the identification of legal persons:

— business name;

— legal form;

— place of head office;

(iii) information for the identification of both natural and legal persons:

— telephone numbers;

— email addresses;

— details of accounts held with banks or other financial institutions;

— status in the proceedings;

(iv) information on the offence:

— information concerning legal persons involved in the preparation or commission of a terrorist offence;

— legal qualification of the offence under national law;

— applicable form of serious crime from the list referred to in Annex I;

— any affiliation with a terrorist group;

— type of terrorism, such as jihadist, separatist, left-wing or right-wing;

— brief summary of the case;

(v) information on the national proceedings:

— status of such proceedings;

— responsible public prosecutor's office;

— case number;

— date of opening of formal judicial proceedings;

— links with other relevant cases;

(vi) additional information field (free text);

(vii) prior authorisation code.

2.2.2. Data transmitted in accordance with Article 21 of Regulation (EU) 2018/1727

(a) Article 21(4) of Regulation (EU) 2018/1727, setting up of joint investigation teams ('JITs')

(i) Top-level section

This top-level section corresponds to the information set out in Article 21(4) of Regulation (EU) 2018/1727 information on the setting up of JITs.

(ii) Structure of the message

The structure of the data shall consist of a sequence of elements and include the following as a minimum:

— National judicial authority in charge of the criminal proceedings

— National reference number of the criminal proceedings

— Status of the criminal proceedings

— Criminal offences investigated

— Other countries involved in the case

— Case already supported by Eurojust?

— If yes, Eurojust case ID?

— If no, is this a request for support?

— Case supported by Europol?

— If yes, operational task force ('OTF') and/or Secure Information Exchange Network Application ('SIENA')?

— JIT agreement:

— Countries involved

— JIT parties (national authorities in charge of the investigations)

— National reference number of the criminal proceedings covered by the JIT

— Date of signature

— Duration

— Criminal offences investigated

— Brief summary of the case

— Main suspects in the criminal proceedings covered by the JIT (name, surname, date and place of birth and possibly other relevant and necessary categories of data under Annex II)

— Results of the work of the JITs:

— Difficulties/delays in:

— setting up the JIT

— requesting/sharing evidence within the JIT

— agreeing on/implementing a common prosecution strategy

— Admissibility/inadmissibility/evaluation of JIT evidence in national proceedings

— Outcome of judicial proceedings (successful/unsuccessful prosecutions and convictions/acquittals)

(iii) Prior authorisation code

(b) Article 21(5) of Regulation (EU) 2018/1727, serious complex cases

(i) Top-level section

This top-level section corresponds to the information set out in Article 21(5) of the Eurojust Regulation, i.e. serious complex cases.

(ii) Structure of the message

The structure of the data shall consist of a sequence of elements and include the following as a minimum:

— National judicial authority in charge of the criminal proceedings

— National reference number of the criminal proceedings

— Status of the criminal proceedings

— Criminal offences investigated

— Other countries involved in the case

— Case already supported by Eurojust?

— If yes, Eurojust case ID?

— If no, is this a request for support?

- Case supported by Europol?
  - If yes, operational task force and/or SIENA?
- Applicable form of serious crime
- Involvement of an organised crime network
  - Mafia type
  - Transnational organised crime network
- Repercussions at EU level
- Main suspects in the criminal proceedings (name, surname, date and place of birth and possibly other relevant and necessary categories of data under Annex II)
- Brief summary of the case
- Other countries involved
  - Countries with which cooperation already initiated
    - Competent authorities involved in other country
    - Judicial cooperation instruments used
    - Number of requests sent/received
    - Existence of linked investigations
  - Countries with which cooperation to be activated/countries possibly affected
    - Type of cooperation needed (such as. extradition, evidence gathering, other cooperation)
  - Existence of linked investigations

(iii) Prior authorisation code

(c) Article 21(6), point (a), of Regulation (EU) 2018/1727, conflicts of jurisdiction

(i) Top-level section

This top-level section corresponds to the information set out in Article 21(6), point (a) of Regulation (EU) 2018/1727, i.e. conflicts of jurisdiction.

(ii) Structure of the message

The structure of the data shall consist of a sequence of elements and include the following as a minimum:

- National judicial authority in charge of the criminal proceedings
- National reference number of the criminal proceedings
- Status of the criminal proceedings (e.g. investigation, prosecution, trial)
- Criminal offences investigated
- Other countries involved in the case
- Case already supported by Eurojust?
  - If yes, Eurojust case ID?
  - If no, is this a request for support?

— Case supported by Europol?

— If yes, operational task force and/or SIENA?

— Other countries involved

— Competent national authorities in the other country, if known

— National reference number of criminal proceedings in other country

— Stage of proceedings in other country, if known

— Positive or negative conflict

— Actual or potential conflict

— Coordination activities already undertaken (e.g. consultations under Council Framework Decision 2009/948/JHA ([1]))

— Brief summary of the case

— Main common suspects (name, surname, date and place of birth and possibly other relevant and necessary categories of data under Annex II)

(iii) Prior authorisation code

(d) Article 21(6), point (b), controlled deliveries

(i) Top-level section

This top-level section corresponds to the information set out in Article 21(6), point (b) of Regulation (EU) 2018/1727: controlled deliveries.

(ii) Structure of the message

The structure for the data shall consist of a sequence of elements and include the following as a minimum:

— National judicial authority in charge of the criminal proceedings

— National reference number of the criminal proceedings

— Status of the criminal proceedings (e.g. investigation, prosecution, trial)

— Criminal offences investigated

— Other countries involved in the case

— Case already supported by Eurojust?

— If yes, Eurojust case ID?

— If no, is this a request for support?

— Case supported by Europol?

— If yes, operational task force and/or SIENA?

— Other countries involved

— Country of origin/transit/destination

— Competent national authorities in other countries

— Existence of linked investigations in other countries

([1]) Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJ L 328, 15.12.2009, p. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Type of goods delivered (e.g. drugs and type/money/weapons/cigarettes/other)

— Status of the controlled delivery (e.g. planned, ongoing, completed)

— Outcome of the controlled delivery, if already executed

— Judicial cooperation instrument used

— Main common suspects (name, surname, date and place of birth and possibly other relevant and necessary categories of data under Annex II)

(iii) Prior authorisation code

(e) Article 21(6), point (c), of Regulation (EU) 2018/1727, repeated issues with judicial cooperation instruments

(i) Top-level section

This top-level section corresponds to the information set out in Article 21(6), point (c) of Regulation (EU) 2018/1727: repeated issues with judicial cooperation instruments.

(ii) Structure of the message

The structure of the data shall consist of a sequence of elements and include the following as a minimum:

— National judicial authority in charge of the criminal proceedings

— National reference number of the criminal proceedings

— Status of the criminal proceedings (e.g. investigation, prosecution, trial)

— Criminal offences investigated

— Other countries involved in the case

— Case already supported by Eurojust?

— If yes, Eurojust case ID?

— If no, is this a request for support?

— Case supported by Europol?

— If yes, operational task force and/or SIENA?

— Other countries involved

— Competent national authorities, if known

— Acting as issuing or executing authority

— Judicial cooperation instrument involved (e.g. EAW, EIO, freezing and confiscation)

— Specific request concerned (i.e. what investigative measure, what type of freezing, EAW for execution of sentence or for prosecution)

— Refusal or repeated difficulty

— If refusal, what specific ground invoked?

— Brief description of the issue

— Other national authorities affected by the same issue, if any

(iii) Prior authorisation code

2.3. *Prior authorisation codes*

When sharing data with Eurojust through JUDEX, the competent national authorities shall indicate via prior authorisation codes the further handling, access and transfer of data following identification of a link. The prior authorisation codes shall indicate whether and to what extent information related to the link may be shared with other competent national authorities, other Union agencies and bodies, third countries or international organisations.

2.4. *Predefined messages*

Predefined messages are representations of exchanges established by Regulation (EU) 2018/1727, but for which no specific form was provided in the legal act. Their types and number are determined during the business and technical analysis.

The XLM Schema Definitions (XSD) for predefined messages shall be designed to ensure consistency, structure, and compliance with business needs.

The following shall apply to those schemas:

(a) the Top-level Section in this schema shall be named according to the specific message type being defined;

(b) the necessary fields required for the specific message type shall be added and defined within this structure, ensuring proper representation of data elements.

2.5. *Free text messages*

Free text messages are representations of exchanges that allow for unstructured or partially structured content, enabling flexibility while still adhering to regulatory and business requirements. The XSD for free text messages shall be designed to ensure consistency and proper formatting.

The following shall apply those schemas.

(a) the Top-level Section in the schema shall be named according to the specific free text message type being defined;

(b) the schema shall define the necessary structure for the free text message while allowing for appropriate ordering of elements as required;

(c) the necessary fields required for the specific free text message type shall be added and defined within this structure, ensuring proper representation of data element.

ANNEX III

TECHNICAL SPECIFICATIONS OF FINGERPRINTS AND PHOTOGRAPHS

Messages exchanged through the decentralised IT system may be accompanied by attachments, including by National Institute of Standards and Technology ('NIST') files containing fingerprints and photographs, in accordance with the technical specifications set out in points 1 and 2.

1. **Fingerprints**

The fingerprints which may be shared with Eurojust for the purpose of reliably identifying individuals subject to criminal proceedings related to terrorism offences, shall meet the following conditions:

(a) the fingerprints are provided in one file containing fingerprint digital images (the fingerprints NIST file) and are submitted in accordance with the ANSI/NIST-ITL 1-2011 Update 2015 standard (or newer version);

(b) the fingerprints NIST file consists of up to ten individual fingerprints: rolled, flat or both;

(c) all fingerprints are labelled;

(d) the fingerprints are captured by live scans or inked on paper, provided that the fingerprints inked on paper have been scanned in the required resolution and with the same quality;

(e) the fingerprints NIST file allows for the inclusion of complementary information such as the conditions of fingerprint registration and the method used for acquiring individual fingerprint images;

(f) the fingerprints have a nominal resolution of either 500 or 1 000 ppi [1] (with an acceptable deviation of +/– 10 ppi) with 256 grey levels;

(g) the fingerprints compression algorithm to be used follows the recommendations of National Institute of Standards and Technology ('NIST'). Fingerprint data with a resolution of 500 ppi is compressed using the WSQ algorithm (ISO/IEC 19794-5:2005). Fingerprint data with a resolution of 1 000 ppi is compressed using the JPEG 2000 image compression standard (ISO/IEC 15444-1) and coding system. The target compression ratio is 15:1.

2. **Photographs**

The photographs which may be shared with Eurojust for the purpose of reliably identifying individuals subject to criminal proceedings related to terrorism offences, shall meet the following conditions:

(a) only one facial image is provided in a photograph file (the photograph NIST file) and is submitted in accordance with the ANSI/NIST-ITL 1-2011 Update 2015 standard, or any newer version available;

(b) the photographs are either grayscale, colour or near infrared;

(c) the quality of the photographs is based on the image requirements of ISO/IEC 19794-5:2011 Frontal image type, or any newer version available;

(d) the photograph NIST file allows the inclusion of complementary information, including the date when the image was taken;

[1] Pixels per inch.

(e) the photographs, in portrait mode, are at a minimum resolution of 600 pixels by 800 pixels and a maximum resolution of 1 200 pixels by 1 600 pixels;

(f) the face occupies a space within the photograph which ensures a minimum of 120 pixels between the centre of each eye;

(g) the photographs compression algorithm used follows the recommendations of the National Institute of Standards and Technology ('NIST'). Photographs are compressed only once with JPG (ISO/IEC 10918) or JPEG 2000 (ISO/IEC 15444) image compression standard and coding system, at a 20:1 maximum allowed image compression ratio.