2026/101

16.1.2026

COMMISSION IMPLEMENTING REGULATION (EU) 2026/101

of 15 January 2026

on setting out the technical specifications and other requirements for the decentralised IT system, as referenced in Regulation (EU) 2023/2844 of the European Parliament and of the Council, in relation to the procedures established by the legal acts listed in points 3 and 4 of Annex I, the legal acts listed in points 1, 10 and 11 of Annex II to that Regulation, and to the procedure established by Article 19a of Regulation (EU) 2020/1784 of the European Parliament and of the Council, as introduced by Article 24(3) of Regulation (EU) 2023/2844 of the European Parliament and of the Council for the electronic service of documents through the European electronic access point

THE EUROPEAN COMMISSION,

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

Having regard to 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 ([1]), and in particular Article 10(1), thereof,

Whereas:

(1) In order to ensure secure, efficient, swift, interoperable, confidential and reliable communication between Member States for the purposes of cross-border judicial procedures in civil, commercial and criminal matters, appropriate communication technology should be used, provided that certain conditions relating to the security, integrity and reliability of the document received and the identification of the participants in the communication are met. The decentralised IT system referred to in Regulation (EU) 2023/2844 should be used by default in the communication between competent authorities.

(2) This decentralised IT system should be comprised of back-end systems in the Member States and the relevant Union bodies and agencies, as well as interoperable access points through which those systems are linked using secure interconnections.

(3) Regulation (EU) 2023/2844 mandates the use of qualified electronic signatures and seals as well as electronic identification means with assurance level high. To meet this obligation, it is necessary to ensure that the decentralised IT system is able to operate with qualified electronic signatures, seals, and electronic identification means, such as the European Digital Identity Wallets established pursuant to Regulation (EU) No 910/2014 ([2]) ('EU Digital Identity Framework').

(4) Regulation (EU) 2022/850 of the European Parliament and of the Council ([3]) establishes the e-Justice Communication via the Online Data Exchange (e-CODEX) system, which is a tool developed to ensure direct, interoperable, sustainable, reliable and secure cross-border electronic exchange of case-related data between competent authorities. The access points of the decentralised IT system should be based on e-CODEX.

(5) The decentralised IT system under Regulation (EU) 2023/2844 is implemented within a larger e-CODEX-based decentralised IT system referred to as the JUstice Digital EXchange System (JUDEX) requiring an effective exchange of information concerning horizontal developments.

(6) It is necessary to lay down rules to enable Member States as well as Union bodies and agencies to adapt their relevant IT systems for the purpose of connection to the decentralised IT system.

([1]) OJ L 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/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) 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).

(7) Member States should also be able to use software developed by the Commission (reference implementation software) instead of a national IT system. In order to ensure interoperability with national IT systems, the reference implementation software should be able to implement the digital procedural standards, as defined in Regulation (EU) 2022/850.

(8) Digital procedural standards, as defined in Regulation (EU) 2022/850, should be implemented by the national back-end systems and the authorised e-CODEX access points for the purposes of and in order to support electronic communication for the procedures established by the legal acts listed in points 3 and 4 of Annex I and the legal acts listed in points 1, 10 and 11 of Annex II to Regulation (EU) 2023/2844 and the procedure established by Article 19a of Regulation (EU) 2020/1784 of the European Parliament and of the Council ([4]), as introduced by Article 24(3) of Regulation (EU) 2023/2844 for the electronic service of documents through the European electronic access point.

(9) Nothing in this Regulation should be interpreted as derogating from the provisions of legal acts listed in Article 1.

(10) In accordance with Commission Decision (EU) 2024/789 ([5]), Ireland participates in this Regulation only in relation to the legal acts listed in Annexes I and II to Regulation (EU) 2023/2844 in which Ireland participates and by which it is bound. In accordance with Article 3 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the 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 their wish to take part in the adoption and application of Regulation (EU) 2020/1784.

(11) 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 is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(12) 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 ([6]) and delivered an opinion on 28 November 2025.

(13) The measures provided for in this Regulation are in accordance with the opinion of the Digitalisation of Judicial Cooperation Committee,

HAS ADOPTED THIS REGULATION:

Article 1

Scope

This Regulation applies to:

(1) Electronic communications in the procedures established by:

(a) Regulation (EC) No 1896/2006 of the European Parliament and of the Council ([7]).

(b) Regulation (EC) No 861/2007 of the European Parliament and of the Council ([8]).

([4]) Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) (OJ L 405, 2.12.2020, p. 40, ELI: http://data.europa.eu/eli/reg/2020/1784/oj).

([5]) Commission Decision (EU) 2024/789 of 6 March 2024 on confirming the participation of Ireland in Regulation (EU) 2023/2844 of the European Parliament and of the Council on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters (OJ L, 2024/789, 8.3.2024, ELI: http://data.europa.eu/eli/dec/2024/789/oj).

([6]) 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).

([7]) Regulation (EC) No 1896/2006 of the European Parliament and of the Council of 12 December 2006 creating a European order for payment procedure (OJ L 399, 30.12.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/1896/oj).

([8]) Regulation (EC) No 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure (OJ L 199, 31.7.2007, p. 1, ELI: http://data.europa.eu/eli/reg/2007/861/oj).

(c) Council Framework Decision 2002/584/JHA ([9]).

(d) Directive 2014/41/EU of the European Parliament and of the Council ([10]).

(e) Regulation (EU) 2018/1805 of the European Parliament and of the Council ([11]).

(2) Electronic communications in the procedure established by Article 19a of Regulation (EU) 2020/1784, as introduced by Article 24(3) of Regulation (EU) 2023/2844 for the electronic service of documents through the European electronic access point.

Article 2

Technical specifications of the decentralised IT system

The technical specifications, measures and objectives of the decentralised IT system, referred to in Article 10(1), points (a), (b), (c) and (d), of Regulation (EU) 2023/2844 shall be as set out in Annex I to this Regulation.

Article 3

Digital procedural standard for the procedure under Regulation (EC) 1896/2006

The digital procedural standard applicable to electronic communication through the decentralised IT system in the procedure under Regulation (EC) No 1896/2006 shall be as set out in Annex II to this Regulation.

Article 4

Digital procedural standard for the procedure under Regulation (EC) No 861/2007

The digital procedural standard applicable to electronic communication through the decentralised IT system in the procedure under Regulation (EC) No 861/2007 shall be as set out in Annex III to this Regulation.

Article 5

Digital procedural standard for the procedures under Framework Decision 2002/584/JHA

The digital procedural standard applicable to electronic communication through the decentralised IT system in procedures under Framework Decision 2002/584/JHA shall be as set out in Annex IV to this Regulation.

([9]) Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States – Statements made by certain Member States on the adoption of the Framework Decision (OJ L 190, 18.7.2002, p. 1, ELI: http://data.europa.eu/eli/dec_framw/2002/584/oj).

([10]) Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1, ELI: http://data.europa.eu/eli/dir/2014/41/oj).

([11]) Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders (OJ L 303, 28.11.2018, p. 1, ELI: http://data.europa.eu/eli/reg/2018/1805/oj).

Article 6

Digital procedural standard for the procedures under Directive 2014/41/EU

The digital procedural standard applicable to electronic communication through the decentralised IT system in procedures under Directive 2014/41/EU shall be as set out in Annex V to this Regulation.

Article 7

Digital procedural standard for the procedures under Regulation (EU) 2018/1805

The digital procedural standard applicable to electronic communication through the decentralised IT system in procedures under Regulation (EU) 2018/1805 shall be as set out in Annex VI to this Regulation.

Article 8

Digital procedural standard for the procedure under Article 19a of Regulation (EU) 2020/1784, as introduced by Article 24(3) of Regulation (EU) 2023/2844

The digital procedural standard applicable to electronic communication through the decentralised IT system in the procedure established by Article 19a of Regulation (EU) 2020/1784, as introduced by Article 24(3) of Regulation (EU) 2023/2844 for the electronic service of documents through the European electronic access point shall be as set out in Annex VII to this Regulation.

Article 9

Implementation timetable

The implementation timetable referred to in Article 10(1), point (f), of Regulation (EU) 2023/2844 shall be as set out in Annex VIII of this Regulation.

Article 10

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, 15 January 2026.

For the Commission
The President
Ursula VON DER LEYEN

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 in accordance with Regulation (EU) 2023/2844 for the legal acts listed in points 3 and 4 of Annex I, the legal acts listed in points 1, 10 and 11 of Annex II to that Regulation, and the procedure established by Article 24(3) of Regulation (EU) 2023/2844 for the electronic service of documents through the European electronic access point.

2. **Definitions**

2.1. 'Data exchange' means the exchange of messages and documents through the decentralised IT system;

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

2.3. '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;

2.4. '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, and electronic signatures and electronic seals;

2.5. 'REST' (REpresentational State Transfer) is an architectural style for designing networked applications. It relies on a stateless, client-server communication model and uses standard methods to perform operations on resources, which are typically represented in structured formats;

2.6. 'SOAP' 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;

2.7. 'Web service' means a software system designed to support interoperable machine-to-machine interaction over a network; it has an interface described in a machine-processable format.

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

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.

Specifically, it shall involve communication through e-CODEX access points, as set out in Article 5(2) of Regulation (EU) 2022/850.

4. **Communication protocols**

The decentralised IT system shall use secure internet protocols, such as HTTPS, for communication within the decentralised IT system, and standards-based communication protocols, such as SOAP or methods, such as REST, for the transmission of structured data and metadata.

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:

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

(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. 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;

5.3. To the extent possible, Public Key Infrastructure (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. 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;

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

5.5. 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 pursuant to respectively Regulation (EU) 2016/679 of the European Parliament and of the Council ([2]) and Directive (EU) 2016/680 of the European Parliament and of the Council ([3]), as applicable;

5.6. Member States which use a national IT system different than the reference implementation software shall implement the necessary measures to ensure that it complies with the requirements of Regulation (EU) 2016/679 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, and support data controllers in fulfilling their accountability obligations.

([2]) 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).

([3]) 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).

5.7. Having regard to their participation in the decentralised IT system, Eurojust and the European Public Prosecutor's Office shall implement the necessary measures to ensure that their respective IT systems comply with the requirements of Regulation (EU) 2018/1725 and their founding acts;

5.8. For the IT systems part of the decentralised IT system under their responsibility, Member States, Eurojust and the European Public Prosecutor's Office 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.

6. **Minimum availability objectives**

6.1. 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 annual basis, excluding scheduled maintenance;

6.2. The Commission shall ensure 24 hours, 7 days a week availability of the Competent courts (authorities) database (CDB), with a target technical availability rate of more than 99 % on annual basis, excluding scheduled maintenance;

6.3. To the extent possible, maintenance operations shall be planned outside of working days or during working days between 20:00h-7:00h CET;

6.4. Member States shall notify the Commission 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 and the other Member States of the time and day(s) when such fixed regular windows are planned. Without affecting the obligations set out in point 6.4, if components of the decentralised IT system under 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 case of unexpected technical failure of the components of the decentralised IT system under Member States' responsibility, Member States shall inform the Commission and the other Member States about it without delay, and, if known, of the projected recovery timeframe;

6.7. In case of unexpected technical failure of the Competent courts (authorities) database (CDB), the Commission shall inform the Member States without delay of the unavailability, and if known, of the projected recovery timeframe;

6.8. Member States shall ensure the availability of data, including personal data, processed within the components of the decentralised IT system under their responsibility. Appropriate technical and organisational measures shall be implemented to prevent data loss and to ensure the timely restoration of access to data in case of an incident. Such measures may include, as appropriate, a backup and recovery policy, regular testing of backup integrity and restoration procedures, and data storage redundancy mechanisms.

7. **Competent courts (authorities) database (CDB)** ([4])

7.1. In accordance with Article 3(1) of Regulation (EU) 2023/2844, the decentralised IT system shall enable electronic communication between the competent authorities, as defined in Article 2(1) thereof, of different Member States and between a national competent authority and a Union body or agency. Pursuant to Article 3(6) of that Regulation, a Member State may also decide to use the decentralised IT system for communication between its national authorities. Moreover, the decentralised IT system shall, pursuant to Article 4 of Regulation (EU) 2023/2844, enable direct electronic communication between natural or legal persons or their representatives, and the competent authorities in the context of Regulations (EC) No 1896/2006 and (EC) No 861/2007.

Therefore, taking into account Member States' obligations to notify and update the list of their competent authorities as set out in the relevant provisions of the legal acts referred to in Article 1 of this Regulation, and in accordance with Article 17(1), point (e), of Regulation (EU) 2023/2844, it is essential to establish an authoritative database of information regarding those authorities for the purposes of the decentralised IT system;

7.2. The authoritative database of the competent authorities shall include the following information in a structured format:

(a) for the purposes of Article 4(2), point (a), and, where applicable, Article 3(6) of Regulation (EU) 2023/2844, information on the competent authorities pursuant to Regulation (EC) No 1896/2006, notably Article 29(1) thereof, as well as those subject to additional notifications under Article 17(1), point (e), of Regulation (EU) 2023/2844;

(b) for the purposes of Article 4(2), point (a), and, where applicable, Article 3(6) of Regulation (EU) 2023/2844, information on the competent authorities pursuant to Regulation (EC) 861/2007, notably Article 25(1) thereof, as well as those subject to additional notifications under Article 17(1), point (e), of Regulation (EU) 2023/2844;

(c) for the purposes of Article 3(1) and, where applicable, Article 3(6) of Regulation (EU) 2023/2844, information on the authorities notified pursuant to Council Framework Decision 2002/584/JHA, notably Articles 6(3), Article 7(2) and 25(2) thereof, as well as those subject to additional notifications under Article 17(1), point (e), of Regulation (EU) 2023/2844;

(d) for the purposes of Article 3(1) and, where applicable, Article 3(6) of Regulation (EU) 2023/2844, information on the authorities notified pursuant to Directive 2014/41/EU, notably Article 33(1), points (a) and (c), thereof, as well as those subject to additional notifications under Article 17(1), point (e), of Regulation (EU) 2023/2844;

(e) for the purposes of Article 3(1) and, where applicable, Article 3(6) of Regulation (EU) 2023/2844, information on the authorities notified pursuant to Regulation (EU) 2018/1805, notably Article 24(1) and (2) thereof, as well as those subject to additional notifications under Article 17(1), point (e), of Regulation (EU) 2023/2844;

(f) for the purposes of Article 4(4) and Article 24(3) of Regulation (EU) 2023/2844 information on the competent authorities subject to additional notifications under Article 17(1), point (e), of Regulation (EU) 2023/2844 for the purposes of Article 19a of Regulation (EU) 2020/1784;

(g) The authorities referred to in points (c) to (e) shall include:

(i) Eurojust national members, including with regard to where, pursuant to Article 8(3) and (4) of Regulation (EU) 2018/1727 of the European Parliament and of the Council ([5]), in accordance with national law they may issue or execute a request for mutual legal assistance or mutual recognition, or order, request or execute investigative measures, as provided for in Directive 2014/41/EU;

([4]) For historical reasons, the system is named the 'Competent Courts Database'. However, to provide better clarity, the authoritative database will also include information on other types of authorities, such as prosecution offices, bailiffs and ministries of justice.

([5]) Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (OJ L 295, 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj).

(ii) With regard to Council Framework Decision 2002/584/JHA, the European Delegated Prosecutors, in the meaning of Article 33(2) of Regulation (EU) 2017/1939 of the European Parliament and of the Council ([6]);

(iii) The European Delegated Prosecutors and the European Prosecutors, where notified by Member States in accordance with Article 105(3) of Regulation (EU) 2017/1939 as competent issuing or executing authorities (or both).

(h) the necessary information to enable communication with the EPPO's Central Office via the decentralised IT system, where applicable;

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

(j) 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 authoritative database.

7.4. The Competent courts (authorities) database (CDB) shall enable Member States to update the information therein and the authorities participating in the decentralised IT system to programmatically access and retrieve information.

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

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

([6]) Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

ANNEX II

Digital procedural standard for the digitalisation of Regulation (EC) No 1896/2006

1. **Introduction and scope**

Article 3(9) of Regulation (EU) 2022/850 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) defines 'digital procedural standard' 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 access points. The business process model shall be developed, maintained and updated applying the Business Process Model and Notation (BPMN) or other industry-wide standards for business process modelling.

The data schemas shall allow for interoperable data exchanges through e-CODEX.

Therefore, for the purposes of the digitalisation of Regulation (EC) No 1896/2006, this Annex shall set out the technical specifications for:

(a) business process models,

(b) data schemas.

2. **Technical specifications for the business process models under Regulation (EC) No 1896/2006**

The technical specifications for business process models shall be considered minimum specifications and shall set out the key aspects necessary for enabling electronic communication for the purposes of Regulation (EC) No 1896/2006 through the decentralised IT system, and shall include both cross-border communication instances and, where Member States choose to utilise the decentralised IT system for that purpose, those between national actors (e.g. in case of a forward to another competent court or authority).

They shall be as follows:

Request for the European Order for Payment Process

— Submit an application – The claimant sends Form A to the Court;

— Request by the Court to the claimant to complete and/or rectify the application form – The Court sends Form B to the claimant;

— Proposal to the claimant to modify the application for an EOP – The Court sends Form C to the claimant;

— The Court rejects the application – The Court sends Form D to the claimant;

— The claimant withdraws the application – The claimant communicates to the Court that the application is withdrawn;

— Payments – The parties and the Court communicate regarding the payment of fees;

— Forward to competent Court – The Court forwards the application to the competent Court.

Processing European Order for Payment Process

— Extension of a time limit – The claimant and/or the defendant request an extension of a time limit set by the Court and the Court communicates a decision on the request;

— The Court issues and serves the EOP on the defendant – The Court issues and serves the EOP (Form E) upon the defendant;

— The defendant opposes the EOP – The defendant submits a statement of opposition to the EOP (Form F) to the Court.

Post- EOP

— The Court sends to claimant the declaration that the EOP is enforceable – The Court sends to the claimant the declaration of enforceability (Form G);

— Appeal – The claimant or the defendant may file an appeal, if possible under national law;

— Review – The defendant applies for review in exceptional cases.

3. Technical specifications for data schemas

The following paragraphs outline the provisions for the technical specifications that shall serve as a basis for developing XML Schema Definitions (XSDs). 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 changes to these specifications.

The specifications are provided for the statutory forms, predefined messages or free text messages used in the exchanges under Regulation (EC) 1896/2006.

3.1. General Considerations

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

Versioning

A version attribute shall be included to facilitate schema versioning management. This will allow to update the schema in future iterations as per the business requirements, indicating whether the new version is backward compatible when introducing new features or refinements.

Schema Declaration and Metadata

Where applicable, the schema shall make use of relevant standards or vocabularies, applied 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.

Annotations and Documentation

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

Usage and Adaptability

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.

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.

Adaptable Structure: The schema shall be designed with the purpose of allowing for the addition or modification of elements or data types as necessary. The form's structure may accommodate changes in requirements without major redesigns.

Optional Elements: Elements within a form may be marked as optional, meaning 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.

Modifications

The schema design shall emphasise flexibility, modularity, and ease of adaptation. The use of complex types and optional elements shall ensure that it may handle diverse scenarios while remaining easy to modify and extend.

3.2. **Statutory Forms**

The technical specifications for the data schemas shall define a structured framework for representing the forms, as set out by Regulation (EC) 1896/2006, in XML format.

3.3. **Predefined messages**

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

Their schemas shall be designed to define a structure of XML Schema Definitions (XSD) ensuring consistency, structure, and compliance with business needs.

The outline of the key components of these schemas shall be the following:

— The Top-level Section in this schema shall be named according to the specific message type being defined.

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

3.4. **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. This schema is designed to define the structure of XML Schema Definitions (XSD) for these messages, ensuring consistency and proper formatting.

The outline of the key components of these schemas shall be the following:

— The Top-level Section in this schema shall be named according to the specific free text message type being defined.

— The schema shall define the necessary structure for the free text message while allowing for appropriate ordering of elements as required.

— The necessary fields required for the specific free text message type will be added and defined within this structure, ensuring proper representation of data elements.

ANNEX III

Digital procedural standard for the digitalisation of Regulation (EC) No 861/2007

1. **Introduction and scope**

Article 3(9) of Regulation (EU) 2022/850 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) defines 'digital procedural standard' 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 access points. The business process model shall be developed, maintained and updated applying the Business Process Model and Notation (BPMN) or other industry-wide standards for business process modelling.

The data schemas shall allow for interoperable data exchanges through e-CODEX.

Therefore, for the purposes of the digitalisation of Regulation (EC) No 861/2007, this Annex shall set out the technical specifications for:

(a) business process models,

(b) data schemas.

2. **Technical specifications for the business process models under Regulation (EC) 861/2007**

The technical specifications for business process models shall be considered minimum specifications and shall set out the key aspects necessary for enabling electronic communication for the purposes of Regulation (EC) 861/2007 through the decentralised IT system, and shall include both cross-border communication instances and, where Member States choose to utilise the decentralised IT system for that purpose, those between national actors (e.g. in case of a forward to another competent court or authority).

They shall be as follows:

Request for a European Small Claim Process

— Submit a claim – The claimant fills in and submits a claim form (Form A) to the Court;

— The claim is outside the scope of the Regulation – The Court informs the claimant in case the claim is outside the scope of the Regulation;

— Claimant withdraws the claim – The claimant communicates to the Court that the claim is withdrawn;

— Claimant informs the Court that they do not withdraw the claim – the claimant informs the Court that they do not wish to withdraw the claim;

— Request by the Court to complete and/or rectify the claim form – The Court request the claimant (Form B) to complete and/or rectify the claim form;

— Court dismisses the claim –The Court can also dismiss the claim;

— Payments – The parties and the Court communicate regarding the payment of fees;

— Forward to competent Court – The Court forwards the claim to the competent Court.

Processing European Small Claims Process

— The Court serves the claim form on the defendant – The Court serves the claim form and Form C on the defendant;

— The defendant submits a response to the claim – The defendant submits a response to the claim (Form C);

— The defendant submits a counterclaim – The defendant submits a counterclaim (Form A);

— The Court requires translation of a document – The Court requires translation of a document from the claimant or the defendant;

— Oral hearing – The claimant and/or the defendant request an oral hearing which could be decided by the Court, or the Court decides to hold an oral hearing on its own motion;

— Extension of a time limit – The claimant and/or the defendant request an extension of a time limit set by the Court and the Court takes a decision on the request;

— Judgment by the Court – Judgment by the Court to the defendant and the claimant.

Post-judgment

— Appeal – In case an appeal against the judgment is possible under national law, the claimant or the defendant may file an appeal;

— Review of the judgment – The defendant may request a review in exceptional cases and the Court decides on the request for review;

— Request for certificate – The Claimant or the defendant request the certificate (Form D) from the Court.

3. Technical specifications for data schemas

The following paragraphs outline the provisions for the technical specifications that shall serve as a basis for developing XML Schema Definitions (XSDs). 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 changes to these specifications.

The specifications below are provided for the statutory forms, predefined messages or free text messages used in the exchanges under Regulation (EC) 861/2007.

3.1. General Considerations

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

Versioning

A version attribute shall be included to facilitate schema versioning management. This will allow to update the schema in future iterations as per the business requirements, indicating whether the new version is backward compatible when introducing new features or refinements.

Schema Declaration and Metadata

Where applicable, the schema shall make use of relevant standards or vocabularies, applied 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.

Annotations and Documentation

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

Usage and Adaptability

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.

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*.

Adaptable Structure: The schema shall be designed with the purpose of allowing for the addition or modification of elements or data types as necessary. The form's structure may accommodate changes in requirements without major redesigns.

Optional Elements: Elements within a form may be marked as optional, meaning 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.

Modifications

The schema design shall emphasise flexibility, modularity, and ease of adaptation. The use of complex types and optional elements shall ensure that it may handle diverse scenarios while remaining easy to modify and extend.

3.2. **Statutory forms**

The technical specifications for the data schemas shall define a structured framework for representing the forms, as set out by Regulation (EC) 861/2007, in XML format.

3.3. **Predefined messages**

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

Their schemas shall be designed to define a structure of XML Schema Definitions (XSD) ensuring consistency, structure, and compliance with business needs.

The outline of the key components of these schemas shall be the following:

— The top-level element in this schema shall be named according to the specific message type being defined.

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

3.4. **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. This schema is designed to define the structure of XML Schema Definitions (XSD) for these messages, ensuring consistency and proper formatting.

The outline of the key components of these schemas shall be the following:

— The Top-level Section in this schema shall be named according to the specific free text message type being defined.

— The schema shall define the necessary structure for the free text message while allowing for appropriate ordering of elements as required.

— The necessary fields required for the specific free text message type will be added and defined within this structure, ensuring proper representation of data elements.

ANNEX IV

Digital procedural standard for the digitalisation of Framework Decision 2002/584/JHA

1. **Introduction and scope**

Article 3(9) of Regulation (EU) 2022/850 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) defines 'digital procedural standard' 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 access points. The business process model shall be developed, maintained and updated applying the Business Process Model and Notation (BPMN) or other industry-wide standards for business process modelling.

The data schemas shall allow for interoperable data exchanges through e-CODEX.

Therefore, for the purposes of the digitalisation of Framework Decision 2002/584/JHA, this Annex shall set out the technical specifications for:

(a) business process models,

(b) data schemas.

2. **Technical specifications for the business process models under Framework Decision 2002/584/JHA**

The technical specifications for business process models shall be considered minimum specifications and shall set out the key aspects necessary for enabling electronic communication for the purposes of Framework Decision 2002/584/JHA through the decentralised IT system, and shall include both cross-border communication instances and, where Member States choose to utilise the decentralised IT system for that purpose, those between national actors (e.g. in case of a transmission or receipt through a Central Authority, where applicable).

To ensure compliance with Articles 9 and 10 of Framework Decision 2002/584/JHA, the workflows supporting the business process models described below shall account for the possibility of transmitting an EAW outside the decentralised IT system, including via the Schengen Information System (SIS). However, the actual communication process through such channels is out of scope of this Digital Procedural Standard.

The technical specifications for business process models shall be as follows:

Issue and Transmit EAW Process model

The issuing judicial authority issues and sends an EAW to the competent executing judicial authority in the Member State where the requested person is (believed to be) located.

Receive and Execute EAW Process model

Upon receipt of the EAW, the executing judicial authority assesses the request and decides whether to surrender the requested person to the issuing State or to refuse.

Surrender Requested Person Process model

When the executing judicial authority decides to surrender the requested person they inform the issuing State authorities. This business process also addresses conditional surrender and postponement, as well as transit through the territory of another Member State, where applicable.

Refuse to Surrender Requested Person Process model

When an executing judicial authority decides to refuse to surrender the requested person they inform the issuing judicial authority.

Withdraw EAW Process model

If the issuing judicial authority decides to withdraw the EAW, they notify to that effect the executing judicial authority, where the requested person has been deprived of liberty. Withdrawal may take place after the EAW is issued and transmitted until the surrender is effected.

Prosecution for Other Offences Process model

If an issuing judicial authority intends to prosecute a requested person for other offences (cf. Article 27 of Framework Decision 2002/584/JHA), and provided there is no situation of presumed consent pursuant to Article 27(1) of Framework Decision 2002/584/JHA, the issuing judicial authority makes a request in the meaning of Article 27(4) of Framework Decision 2002/584/JHA.

Surrender to a Third Member State Process model

A third Member State may request the surrender of a person, who has been previously surrendered from one Member State to another. In such cases, the last executing State of the EAW must provide its consent.

Extradition to a Third Country Process model

In accordance with Article 28(4) a person surrendered on the basis of an EAW cannot be extradited to a third State without the consent of the authority of the Member State, which has surrendered the person.

3. Technical specifications for data schemas

The following paragraphs outline the provisions for the technical specifications that shall serve as a basis for developing XML Schema Definitions (XSDs) for the digitalisation of Framework Decision 2002/584/JHA. 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 changes to these specifications.

The specifications are provided for the statutory form annexed to Framework Decision 2002/584/JHA, any predefined message, or free text messages used in exchanges under Framework Decision 2002/584/JHA.

3.1. General Considerations

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

Versioning

A version attribute shall be included to facilitate schema versioning management. This will allow to update the schema in future iterations as per the business requirements, indicating whether the new version is backward compatible when introducing new features or refinements.

Schema Declaration and Metadata

Where applicable, the schema shall make use of relevant standards or vocabularies, applied 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

— Aggregated Components

— 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.

Annotations and Documentation

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

Usage and Adaptability

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.

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.

Adaptable Structure: The schema shall be designed with the purpose of allowing for the addition or modification of elements or data types as necessary. The form's structure may accommodate changes in requirements without major redesigns.

Optional Elements: Elements within a form may be marked as optional, meaning 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.

Modifications

The schema design shall emphasise flexibility, modularity and ease of adaptation. The use of complex types and optional elements shall ensure that it may handle diverse scenarios while remaining easy to modify and extend.

3.2. Statutory Forms

The technical specifications for the data schemas shall define a structured framework for representing the forms, as set out by Framework Decision 2002/584/JHA, in XML format.

3.3. Predefined messages

Predefined messages are representations of exchanges established by Framework Decision 2002/584/JHA, but for which no specific form was provided in the legal act. Their types and number will be determined during the business and technical analysis.

Their schemas shall be designed to define a structure of XML Schema Definitions (XSD), ensuring consistency, structure, and compliance with business needs.

The outline of the key components of these schemas shall be the following:

— The top-level element in this schema shall be named according to the specific message type being defined.

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

3.4. 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. This schema is designed to define the structure of XML Schema Definitions (XSDs) for these messages, ensuring consistency and proper formatting.

The outline of the key components of these schemas shall be the following:

— The Top-level Section in this schema shall be named according to the specific free text message type being defined.

— The schema shall define the necessary structure for the free text message while allowing for appropriate ordering of elements as required.

— The necessary fields required for the specific free text message type shall be added and defined within this structure, ensuring proper representation of data elements.

ANNEX V

Digital procedural standard for the digitalisation of Directive 2014/41/EU

1. Introduction and scope

Article 3(9) of Regulation (EU) 2022/850 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) defines 'digital procedural standard' 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 access points. The business process model shall be developed, maintained and updated applying the Business Process Model and Notation (BPMN) or other industry-wide standards for business process modelling.

The data schemas shall allow for interoperable data exchanges through e-CODEX.

Therefore, for the purposes of the digitalisation of Directive 2014/41/EU, this Annex shall set out the technical specifications for:

(a) business process models,

(b) data schemas.

2. Technical specifications for the business process models under Directive 2014/41/EU

The technical specifications for business process models shall be considered minimum specifications and shall set out the key aspects necessary for enabling electronic communication for the purposes of Directive 2014/41/EU through the decentralised IT system, and shall include both cross-border communication instances and, where Member States choose to utilise the decentralised IT system for that purpose, those between national actors (e.g. in case of a transmission or receipt through a Central Authority, where applicable).

They shall be as follows:

2.1. European investigation order

Issue and Transmit EIO Process model

— Issue and Transmit an EIO (Annex A): the Issuing Authority issues an EIO and transmits it to the Executing Authority (where applicable, through the designated Central Authority);

— Provide additional information: the Issuing Authority provides additional information to the Executing Authority (where applicable, through the designated Central Authority);

— Change EIO (Annex A): the Issuing Authority replaces the original EIO with a modified EIO and transmits it to the Executing Authority (where applicable, through the designated Central Authority);

— Issue and transmit supplementary EIO (Annex A): the Issuing Authority issues an EIO which supplements an earlier EIO and transmits it to the Executing Authority (where applicable, through the designated Central Authority);

— Send a notification message: the Issuing Authority sends a notification about the legal remedies sought against the issuing of an EIO to the Executing Authority (where applicable, through the designated Central Authority);

— Withdraw an EIO: the Issuing Authority informs the Executing Authority about withdrawing the EIO in whole (where applicable, through the designated Central Authority);

— Request a status update: the Issuing Authority requests a status update about the evolution of the recognition and execution of an EIO from the Executing Authority (where applicable, through the designated Central Authority);

— Send and receive any other communication needed in the context of an EIO to/from the Executing Authority or where applicable to/from the designated Central Authority.

Receive and Execute EIO Process model

— Receive an EIO and send confirmation of receipt (Annex B): Executing Authority receives the issued EIO from the Issuing Authority and sends confirmation of receipt (where applicable, through the designated Central Authority). In case of a forward of an EIO, this obligation applies both to the authority, which initially received the EIO, including the designated Central Authority, and to the authority to which the EIO was forwarded;

— Forward an EIO and inform the Issuing Authority about the forward (Annex B): if the authority, which received the EIO, is not the competent one or is only partially competent, or if the EIO is received by the designated Central Authority (where applicable), the EIO is forwarded to the competent Executing Authority in the Executing State, and the authority, which forwards the EIO, informs the Issuing Authority about the forward (where applicable, through the designated Central Authority);

— Return an EIO: where an EIO has not been issued by an Issuing Authority as specified under Article 2(c) of Directive 2014/41/EU, the Executing Authority returns the EIO to the Issuing Authority (where applicable, through the designated Central Authority);

— Send a notification message: the Executing Authority notifies the Issuing Authority about a given situation under the following provisions of Directive 2014/41/EU: recital 22, Article 10(4) and (5), Article 12(5) and (6), Article 14(5), Article 15, Article 16(2), points (a), (b) and (c), Article 16(3), point (b), Article 19(2), Article 32(2) and 32(5) (where applicable, through the designated Central Authority);

— Request additional information: Executing Authority requests additional information from the Issuing Authority (where applicable, through the designated Central Authority);

— Inform about the progress of an EIO: the Executing Authority informs the Issuing Authority about the progress of the recognition and execution of the EIO (where applicable, through the designated Central Authority);

— Send the Results of execution of an EIO: the Executing Authority sends the results of the execution of the EIO (either in whole or in part) to the Issuing Authority (where applicable, through the designated Central Authority);

— Refuse an EIO: the Executing Authority informs the Issuing Authority about refusal of EIO (where applicable, through the designated Central Authority);

— Terminate process upon withdrawal of an EIO by the Issuing Authority;

— Send and receive any other communication needed in the context of an EIO to/from the Issuing Authority or, where applicable, to/from the designated Central Authority.

Issue and Transmit Request for Transit Process model

— Issue and Transmit a Request for Transit: the Transit Requesting Authority (an authority of the Issuing State competent to issue a Request for Transit) issues a Request for Transit and transmits it to the Transit Granting Authority (an authority of the Member State of Transit competent to grant transit);

— Provide additional information: the Transit Requesting Authority provides additional information to the Transit Granting Authority;

— Withdraw a Request for Transit: the Transit Requesting Authority informs the Transit Granting Authority about withdrawing the Request for Transit in whole;

— Send and receive any other communication needed in the context of the Request for Transit to/from the Transit Granting Authority.

Receive and Reply to Request for Transit Process model

— Receive a Request for Transit: Transit Granting Authority receives a Request for Transit from the Transit Requesting Authority;

— Forward a Request for Transit: if the authority, which received the Request for Transit, is not the competent one, it forwards the Request for Transit to the competent Transit Granting Authority;

— Request additional information: Transit Granting Authority requests additional information from the Transit Requesting Authority;

— Send a reply to the Request for Transit: Transit Granting Authority sends the reply to the Request for Transit (informing of its decision on whether transit is granted) to the Transit Requesting Authority;

— Terminate process upon withdrawal of the Request for Transit by the Transit Requesting Authority;

— Send and receive any other communication needed in the context of the Request for Transit to/from the Transit Requesting Authority.

2.2. **Interception of Telecommunication Notification (ITN)**

Issue and Transmit ITN Process model

— Issue and Transmit an ITN (Annex C): The Competent Authority of the Intercepting Member State issues a notification about the interception of telecommunication and transmits it to the Competent Authority of the Notified Member State;

— Provide additional information: the Competent Authority of the Intercepting Member State provides additional information to the Competent Authority of the Notified Member State;

— Change ITN (Annex C): the Competent Authority of the Intercepting Member State replaces the original ITN with a modified ITN and transmits it to the Competent Authority of the Notified Member State;

— Withdraw an ITN: the Competent Authority of the Intercepting Member State informs the Competent Authority of the Notified Member State about withdrawing the ITN in whole;

— Send and receive any other communication needed in the context of the ITN to/from the Competent Authority of the Notified Member State.

Receive and Reply to ITN Process model

— Receive an ITN: the Competent Authority of the notified Member State receives an ITN from the Competent Authority of the Intercepting Member State;

— Forward an ITN: if the authority, which received the ITN is not the competent one, it forwards the ITN to the Competent Authority of the Notified Member State;

— Request additional information: the Competent Authority of the notified Member State requests additional information from the Competent Authority of the intercepting Member State;

— Send a notification message: the Competent Authority of the notified Member State sends a notification to the Competent Authority of the Intercepting Member State informing about a decision taken that the interception may not be carried out or shall be terminated, and where necessary that any material already intercepted while the subject of the interception was on its territory may not be used, or may only be used under conditions which it shall specify;

— Terminate process upon withdrawal of the ITN by the Competent Authority of the Intercepting Member State;

— Send and receive any other communication needed in the context of the ITN to/from the Competent Authority of the Intercepting Member State.

3. **Technical specifications for data schemas**

The following paragraphs outline the provisions for the technical specifications that shall serve as a basis for developing XML Schema Definitions (XSDs) for the digitalisation of Directive 2014/41/EU. 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 changes to these specifications.

The specifications are provided for the statutory form, predefined message or free text message used in the exchanges under Directive 2014/41/EU.

3.1. **General Considerations**

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

Versioning

A version attribute shall be included to facilitate schema versioning management. This will allow to update the schema in future iterations as per the business requirements, indicating whether the new version is backward compatible when introducing new features or refinements.

Schema Declaration and Metadata

Where applicable, the schema shall make use of relevant standards or vocabularies, applied 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

— Aggregated Components

— 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.

Annotations and Documentation

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

Usage and Adaptability

Modular Structure: Each section shall be designed with specific functionality and may be reused or adapted independently. This should make the schema easy to customise for different use cases.

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

Adaptable Structure: The schema shall be designed with the purpose of allowing for the addition or modification of elements or data types as necessary. The form's structure may accommodate changes in requirements without major redesigns.

Optional Elements: Many elements within a form may be marked as optional, meaning 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.

Modifications

The schema design shall emphasise flexibility, modularity, and ease of adaptation. The use of complex types and optional elements shall ensure that it may handle diverse scenarios while remaining easy to modify and extend.

3.2. **Statutory Forms**

The technical specifications for the data schemas shall define a structured framework for representing the forms, as set out by Directive 2014/41/EU, in XML format.

3.3. **Predefined messages**

Predefined messages are representations of exchanges established by Directive 2014/41/EU, but for which no specific form was provided in the legal act. Their types and number will be determined during the business and technical analysis.

Their schemas shall be designed to define a structure of XML Schema Definitions (XSD) ensuring consistency, structure, and compliance with business needs.

The outline of the key components of these schemas shall be the following:

— The top-level element in this schema shall be named according to the specific message type being defined.

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

3.4. **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. This schema is designed to define the structure of XML Schema Definitions (XSD) for these messages, ensuring consistency and proper formatting.

The outline of the key components of these schemas shall be the following:

— The Top-level Section in this schema shall be named according to the specific free text message type being defined.

— The schema shall define the necessary structure for the free text message while allowing for appropriate ordering of elements as required.

— The necessary fields required for the specific free text message type shall be added and defined within this structure, ensuring proper representation of data elements.

ANNEX VI

Digital procedural standard for the digitalisation of Regulation (EU) 2018/1805

1. **Introduction and scope**

Article 3(9) of Regulation (EU) 2022/850 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) defines 'digital procedural standard' 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 access points. The business process model shall be developed, maintained and updated applying the Business Process Model and Notation (BPMN) or other industry-wide standards for business process modelling.

The data schemas shall allow for interoperable data exchanges through e-CODEX.

Therefore, for the purposes of the digitalisation of Regulation (EU) 2018/1805, this Annex shall set out the technical specifications for:

(a) business process models,

(b) data schemas.

2. **Technical specifications for the business process models under Regulation (EU) 2018/1805**

The technical specifications for business process models shall be considered minimum specifications and shall set out the key aspects necessary for enabling electronic communication for the purposes of Regulation (EU) 2018/1805 through the decentralised IT system, and shall include both cross-border communication instances and, where Member States choose to utilise the decentralised IT system for that purpose, those between national actors (e.g. in case of a transmission or receipt through a Central Authority, where applicable).

They shall be as follows:

2.1. **Freezing Order (FO)**

Issue and Transmit Freezing Certificate / Order Process model

— Issue and Transmit a Freezing Order: the issuing authority issues a Freezing Order and sends the respective Freezing Certificate (including a (certified) copy of or a digital original of the FO, where so required by the executing State) to the relevant executing authority(ies) (where applicable, through the designated Central Authority).

— Provide additional information: the Issuing Authority provides additional information to the Executing Authority (where applicable, through the designated Central Authority);

— Withdraw a Freezing Order: where the Freezing Order can no longer be recognised and executed or is no longer valid, the issuing authority withdraws the freezing order (where applicable, through the designated Central Authority).

— Reply to Request to Limit the Period of Freezing: The Issuing Authority responds to the request to limit the period of freezing.

— Send and receive any other communication needed in the context of a Freezing Order to/from the Executing Authority or where applicable to/from the designated Central Authority.

Receive and Decide on Freezing Certificate / Order Process model

— Receive a Freezing Order: the Executing Authority receives the Freezing Order (either directly or through a Central Authority of the executing State) and needs to assess the request in order to make a decision on whether to recognise and execute the order.

— Forward a Freezing Order: in case the Freezing Order has been transmitted to a Central Authority of the executing State, that Central Authority forwards the Freezing Order to the correct Executing Authority and informs the Issuing Authority accordingly.

— Request additional information: the Executing Authority requests additional information from the Issuing Authority (where applicable, through the designated Central Authority).

— Extend Time Limits: The Executing Authority informs the Issuing Authority of being unable to meet the time limits (where applicable, through the designated Central Authority).

— Notify about Decision to Recognise and Execute: the Executing Authority recognises a transmitted Freezing Order (either fully or partially). It takes the measures necessary for its execution and informs the Issuing Authority about its decision (where applicable, through the designated Central Authority). Execution can be postponed on one of the statutory grounds.

— Inform about Postponement: the Executing Authority informs the Issuing Authority of the postponement of the Freezing Order (either directly or through a Central Authority).

— Inform about Legal Remedies: the Executing Authority informs the Issuing Authority of invoked legal remedies (either directly or through a Central Authority).

— Send Execution Report: following the successful execution of the Freezing Order, the Executing Authority sends the execution report to the Issuing Authority (either directly or through a Central Authority).

— Request to Limit the Period of Freezing: at any time following the execution of a freezing order, the Executing Authority can send a request to the Issuing Authority to limit the freezing period.

— Notify about the Impossibility to Execute: the Executing Authority notifies the Issuing Authority of the impossibility to execute the Freezing Certificate/Order (either directly or through a Central Authority).

— Notify about Decision not to Recognise and Execute: The Executing Authority inform the Issuing Authority of its decision not to recognise and execute the Freezing Order (either directly or through a Central Authority).

— Terminate process upon withdrawal of a Freezing Order by the Issuing Authority (where applicable, through the designated Central Authority).

— Send and receive any other communication needed in the context of a Freezing Order to/from the Issuing Authority or, where applicable, to/from the designated Central Authority.

2.2. **Confiscation Order (CO)**

Issue and Transmit Confiscation Certificate / Order

— Issue and Transmit Confiscation Order: the issuing authority issues a Confiscation Order and sends the respective Confiscation Certificate (including a copy of or a digital original of the CO, where so required by the executing State) to the relevant executing authority(ies) (where applicable, through the designated Central Authority).

— Provide additional information: the Issuing Authority provides additional information to the Executing Authority (where applicable, through the designated Central Authority).

— Withdraw a Confiscation Order: where the Confiscation Order can no longer be executed or is no longer valid, the issuing authority withdraws the confiscation order (where applicable, through the designated Central Authority).

— Send and receive any other communication needed in the context of a Confiscation Certificate/Order to/from the Executing Authority or where applicable to/from the designated Central Authority.

Receive and Decide on Confiscation Certificate / Order

— Receive a Confiscation Certificate/Order: upon receipt of the Confiscation Order (either directly or through a Central Authority of the executing State) the executing authority assesses the request in view of its recognition and execution.

— Forward a Confiscation Order: in case the Confiscation Order has been transmitted to a Central Authority of the executing State, that Central Authority forwards the Confiscation Order to the correct Executing Authority and informs the Issuing Authority about the forwarding.

— Request additional information: the Executing Authority requests additional information from the Issuing Authority (where applicable, through the designated Central Authority).

— Extend Time Limits: the Executing Authority informs the Issuing Authority of the reasons for not meeting the time limits, and both agree on an appropriate schedule (where applicable, through the designated Central Authority).

— Notify about Decision to Recognise and Execute: the Executing Authority recognises a transmitted confiscation order, it takes the measures necessary for its execution and informs the Issuing Authority about its decision (either directly or through a Central Authority). Execution can be postponed on one of the statutory grounds.

— Inform about Postponement: the Executing Authority informs the Issuing Authority of the postponement of the Confiscation Order (either directly or through a Central Authority).

— Inform about Legal Remedies: the Executing Authority informs the Issuing Authority of invoked legal remedies (either directly or through a Central Authority).

— Send Results on Execution: following the successful execution of the Confiscation Order, the Executing Authority sends the results of the execution to the Issuing Authority (either directly or through a Central Authority).

— Inform about Impossibility to Execute Confiscation Order: the Executing Authority notifies the Issuing Authority of the impossibility to execute the Confiscation Order (where applicable, through the designated Central Authority).

— Notify about decision not to Recognise and/or Execute: the Executing Authority informs the Issuing Authority of its decision not to recognise and execute the Confiscation Order.

— Terminate process upon withdrawal of a Confiscation Order by the Issuing Authority (where applicable, through the designated Central Authority).

— Send and receive any other communication needed in the context of a Confiscation Order to/from the Issuing Authority or, where applicable, to/from the designated Central Authority.

3. **Technical specifications for data schemas**

The following paragraphs outline the provisions for the technical specifications that shall serve as a basis for developing XML Schema Definitions (XSDs) for the digitalisation of Regulation (EU) 2018/1805. 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 changes to these specifications.

The specifications are provided for the statutory forms, any predefined message or free text message used in the exchanges under Regulation (EU) 2018/1805.

3.1. **General Considerations**

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

Versioning

A version attribute shall be included to facilitate schema versioning management. This will allow to update the schema in future iterations as per the business requirements, indicating whether the new version is backward compatible when introducing new features or refinements.

Schema Declaration and Metadata

Where applicable, the schema shall make use of relevant standards and vocabularies, applied 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

— Aggregated Components

— 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.

Annotations and Documentation

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

Usage and Adaptability

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.

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

Adaptable Structure: The schema shall be designed with the purpose of allowing for the addition or modification of elements or data types as necessary. The form's structure may accommodate changes in requirements without major redesigns.

Optional Elements: Elements within the form may be marked as optional, meaning 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.

Modifications

The schema design shall emphasise flexibility, modularity, and ease of adaptation. The use of complex types and optional elements ensures that it may handle diverse scenarios while remaining easy to modify and extend.

3.2. **Statutory Forms**

The technical specifications for the data schemas shall define a structured framework for representing the forms, as set out by Regulation (EU) 2018/1805, in XML format.

3.3. **Predefined messages**

Predefined messages are representations of exchanges established by Regulation (EU) 2018/1805, but for which no specific form was provided in the legal act. Their types and number will be determined during the business and technical analysis.

Their schemas shall be designed to define a structure of XML Schema Definitions (XSD) ensuring consistency, structure, and compliance with business needs.

The outline of the key components of these schemas shall be the following:

— The top-level element in this schema shall be named according to the specific message type being defined.

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

3.4. **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. This schema is designed to define the structure of XML Schema Definitions shall be established for these messages, ensuring consistency and proper formatting.

The outline of the key components of these schemas shall be the following:

— The Top-level Section in this schema shall be named according to the specific free text message type being defined.

— The schema shall define the necessary structure for the free text message while allowing for appropriate ordering of elements as required.

— The necessary fields required for the specific free text message type shall be added and defined within this structure, ensuring proper representation of data elements.

ANNEX VII

Digital procedural standard for the digitalisation of the procedure under Article 19a of Regulation (EU) 2020/1784, as introduced by Article 24(3) of Regulation (EU) 2023/2844

1. **Introduction and scope**

Article 3(9) of Regulation (EU) 2022/850 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) defines 'digital procedural standard' 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 access points. The business process model shall be developed, maintained and updated applying the Business Process Model and Notation (BPMN) or other industry-wide standards for business process modelling.

The data schemas shall allow for interoperable data exchanges through e-CODEX.

Therefore, for the purposes of the digitalisation of the procedure under Article 19a of Regulation (EU) 2020/1784, as introduced by Article 24(3) of Regulation (EU) 2023/2844, this Annex shall set out the technical specifications for:

(a) business process models,

(b) data schemas.

2. **Technical specifications for the business process models under the procedure under Article 19a of Regulation (EU) 2020/1784, as introduced by Article 24(3) of Regulation 2023/2844**

The technical specifications for business process models shall be considered minimum specifications and shall set out the key aspects necessary for enabling electronic communication for the purposes of Article 19a of Regulation (EU) 2020/1784, as introduced by Article 24(3) of Regulation (EU) 2023/2844 through the decentralised IT system, and shall include both cross-border communication instances and, where Member States choose to utilise the decentralised IT system for that purpose, those between national actors.

They shall be as follows:

Service through the EEAP

The Court serves documents to the Addressee through the European Electronic Access Point – The Court serves documents to the Addressee who either acknowledges receipt or refuses service based on the language used.

3. **Technical specifications for data schemas**

The following paragraphs outline the provisions for the technical specifications that shall serve as a basis for developing XML Schema Definitions (XSDs). 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 changes to these specifications.

The specifications below are provided for the statutory forms, predefined messages or free text messages used in the exchanges under the procedure under Article 24(3) of Regulation (EU) 2023/2844.

3.1. **General Considerations**

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

Versioning

A version attribute shall be included to facilitate schema versioning management. This will allow to update the schema in future iterations as per the business requirements, indicating whether the new version is backward compatible when introducing new features or refinements.

Schema Declaration and Metadata

Where applicable, the schema shall make use of relevant standards or vocabularies, applied 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.

Annotations and Documentation

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

Usage and Adaptability

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.

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.

Adaptable Structure: The schema shall be designed with the purpose of allowing for the addition or modification of elements or data types as necessary. The form's structure may accommodate changes in requirements without major redesigns.

Optional Elements: Elements within a form may be marked as optional, meaning 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.

Modifications

The schema design shall emphasise flexibility, modularity, and ease of adaptation. The use of complex types and optional elements shall ensure that it may handle diverse scenarios while remaining easy to modify and extend.

3.2. Statutory forms

The technical specifications for the data schemas shall define a structured framework for representing form L, as set out by the Regulation (EU) 2020/1784, in XML format.

3.3. Predefined messages

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

Their schemas shall be designed to define a structure of XML Schema Definitions (XSD) ensuring consistency, structure, and compliance with business needs.

The outline of the key components of these schemas shall be the following:

— The top-level element in this schema shall be named according to the specific message type being defined.

— The necessary fields required for the specific message type will be added and defined within this structure, ensuring proper representation of data elements.

3.4. **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. This schema is designed to define the structure of XML Schema Definitions (XSD) for these messages, ensuring consistency and proper formatting.

The outline the of key components of these schemas shall be the following:

— The Top-level Section in this schema shall be named according to the specific free text message type being defined.

— The schema shall define the necessary structure for the free text message while allowing for appropriate ordering of elements as required.

— The necessary fields required for the specific free text message type will be added and defined within this structure, ensuring proper representation of data elements.

ANNEX VIII

Implementation timetable

The implementation timetable referred to in Article 10(1), point (f), of Regulation (EU) 2023/2844 is laid down as follows:

(a) A release of the reference implementation software that is fully developed, tested, and stable enough to be deployed in a live environment where end users can access it, including the accompanying documentation, shall be made available by the Commission to the Member States by at the latest four months before the date of application of Articles 3 and 4 of Regulation (EU) 2023/2844, set by Article 26(3) of that Regulation;

(b) Concerning the legal acts in the scope of this implementing Regulation, a release of the Competent courts (authorities) database (CDB) that is fully developed, tested, and stable enough to be deployed in a live environment where end users can access it, including the accompanying documentation, shall be made available by the Commission to the Member States by at the latest four months before the date of application of Articles 3 and 4 of Regulation (EU) 2023/2844, set by Article 26(3) of that Regulation;

(c) Concerning the legal acts in the scope of this implementing Regulation, the data in Competent courts (authorities) database (CDB) shall be fully updated by the Member States as soon as possible but not later than one month before the date of application of Articles 3 and 4 of Regulation (EU) 2023/2844, set by Article 26(3) of that Regulation;

(d) The installation of the reference implementation software by the competent authorities shall be concluded at the latest one month before the date of application of Articles 3 and 4 of Regulation (EU) 2023/2844, set by Article 26(3) of that Regulation;

(e) The adjustments to national IT systems necessary for ensuring compliance with the requirements of the decentralised IT system shall be completed at the latest one month before the date of application of Articles 3 and 4 of Regulation (EU) 2023/2844, set by Article 26(3) of that Regulation.