Official Journal
of the European Union

EN
L series

2025/1550

29.7.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/1550

of 28 July 2025

establishing the technical specifications and other requirements for the decentralised IT system, referred to in Regulation (EU) 2023/1543 of the European Parliament and of the Council

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings ([1]), and in particular Article 25(1), points (a), (b), (c) and (d) thereof,

Whereas:

(1) In order to establish the decentralised IT system referred to in Regulation (EU) 2023/1543, it is necessary to define and adopt technical specifications, measures and objectives for the implementation of that system.

(2) In accordance with Regulation (EU) 2023/1543, the decentralised IT system should be comprised of IT systems of the Member States and the Union agencies and bodies, and interoperable e-CODEX access points through which those IT systems are interconnected. Accordingly, the technical specifications and other requirements of the decentralised IT system should reflect this framework.

(3) In accordance with Regulation (EU) 2023/1543, the access points of the decentralised IT system should be based on authorised e-CODEX access points as defined in Article 3(3) of Regulation (EU) 2022/850 of the European Parliament and of the Council ([2]).

(4) Member States may opt to use the reference implementation software developed by the Commission as their back-end system in place of a national IT system. In order to ensure interoperability, both national IT systems and the reference implementation software should be subject to the same technical specifications and requirements set out in this Regulation.

(5) In order to mitigate potential technical issues related to the capacity and reliability of the decentralised IT system, it is necessary to establish a threshold for the volume of electronic evidence transmitted through that system. Following the system's launch, the frequency and volume of such transmissions should be monitored, and the threshold should be adjusted, where appropriate, to maximise the system's efficiency.

(6) In order to strengthen the interoperability and efficiency of the decentralised IT system the use of appropriate ETSI standards should be mandated. Future developments should be monitored, and, where necessary, the adoption of additional ETSI standards should be considered.

(7) Ireland is bound by Regulation (EU) 2023/1543 and is therefore taking part in the adoption of this Regulation.

(8) 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 bound by or subject to the application of this Regulation.

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

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

(9) 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 ([3]) and delivered an opinion on 25 June 2025.

(10) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 26 of Regulation (EU) 2023/1543,

HAS ADOPTED THIS REGULATION:

Article 1

Technical specifications of the decentralised IT system

The technical specifications and requirements, measures and objectives of the decentralised IT system referred to in Article 25(1) of Regulation (EU) 2023/1543 for communication within the meaning of Article 19 of that Regulation shall be as set out in the Annex to this Regulation.

Article 2

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, 28 July 2025.

For the Commission
The President
Ursula VON DER LEYEN

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

ANNEX

TECHNICAL SPECIFICATIONS OF THE DECENTRALISED IT SYSTEM

(referred to in Article 1)

1. Introduction and scope

This Annex sets out the technical specifications, measures and objectives of the decentralised IT system for the procedures under Regulation (EU) 2023/1543.

According to Regulation (EU) 2023/1543, and in particular its Article 19, the decentralised IT system is to enable written communication between competent authorities and designated establishments or legal representatives, between competent authorities, as well as between competent authorities and competent Union agencies or bodies.

2. Definitions

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

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

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

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

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

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

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

2.8. 'API' means an application programming interface based on a common data exchange standard, allowing service providers who make use of bespoke IT solutions for the purposes of exchanging information and data related to requests for electronic evidence to access the decentralised IT systems by automated means;

2.9. 'web-based interface' means a user interface available over HTTPS on the internet, which allows service providers to access the decentralised IT system manually in order to communicate securely with authorities and to exchange information and data related to requests for electronic evidence, without having to establish their own dedicated infrastructure;

2.10. 'ETSI Standards' means technical specifications and standards developed by the European Telecommunications Standards Institute (ETSI) to ensure interoperability, security, and efficiency in information and communication technologies. They provide frameworks, protocols, and best practices for a wide range of technologies, including mobile networks, radio communications, cybersecurity, and internet infrastructure;

2.11. 'hash digest' means a fixed-length output generated by a cryptographic hash function when applied to an input of arbitrary length. A cryptographic hash function is designed to satisfy fundamental security properties, including preimage resistance, second preimage resistance, and collision resistance, ensuring its robustness against inversion and collision attacks;

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

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

2.14. 'ebMS' means the ebXML Message Service, which is a messaging protocol developed under the OASIS framework that enables secure, reliable, and interoperable exchange of electronic business documents using SOAP, supporting business-to-business integration across diverse systems;

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

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

2.17. Recovery Point Objective means the maximum acceptable amount of data loss in case of failure.

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

3.1. For the purposes of written communication between Member States' competent authorities, between competent authorities and designated establishments or legal representatives of service providers, as well as between competent authorities and Union agencies or bodies, the decentralised IT system shall use service-based methods of communication, such as Web-services or other reusable components and software solutions for data exchange purposes. Specifically, it will involve communication through e-CODEX access points, as set out in Article 5(2) of Regulation (EU) 2022/850. Therefore, to ensure effective and interoperable cross-border data exchange, the decentralised IT system shall support communication via the e-CODEX system.

3.2. Given the anticipated high volume of electronic evidence to be transmitted further to a European Production Order through the decentralised IT system, as outlined in Article 19(1) and (4) of Regulation (EU) 2023/1543, which may lead to technical capacity constraints that could negatively impact the decentralised IT system, electronic evidence shall be transmitted through this system insofar as it does not exceed the threshold of 25 megabytes (25 600 kilobytes). The transmission of electronic evidence exceeding that threshold shall be effected in accordance with Article 19(5) of that Regulation.

3.3. Having regard to Article 19(6) of Regulation (EU) 2023/1543, in case a transmission is effected by alternative means as provided for in that paragraph because of an inability to use the decentralised IT system due to one of the grounds set out in Article 19(5) of that Regulation:

3.3.1. Where the transmission concerns written communication, including the exchange of forms, between competent authorities and service providers in the meaning of Article 19(1) of Regulation (EU) 2023/1543, the originator of the transmission shall record the transmission in its national IT system part of the decentralised IT system. The recorded information shall include as a minimum a case or a file reference number, its date and time, the sender and recipient, the file name and its size.

3.3.2. Where the transmission concerns written communication, including the exchange of forms, between competent authorities, as well as written communication with competent Union agencies or bodies in the meaning of Article 19(4) of Regulation (EU) 2023/1543, the originator of the transmission shall record the transmission in the decentralised IT system, notably within its national IT system or, where applicable, in the IT systems operated by the competent Union agency or body. The recorded information shall include as a minimum a case or a file reference number, the date and time of transmission, the sender and recipient, the file name and its size.

3.3.3. Where electronic evidence pursuant to a European Production Order has been transmitted through alternative means of communication between service providers and the competent authorities in the issuing State ([1]), or where the electronic evidence is transmitted through alternative means from the enforcing authority to the competent authorities in the issuing State under the procedure for enforcement as provided for in Article 16(9) of Regulation (EU) 2023/1543, the originator:

(a) shall record and transmit to the authority to which the electronic evidence has been transmitted or made available the following information as part of a manifest:

(1) information on the sender and the recipient;

(2) metadata associating the provided electronic evidence with a particular European Production or Preservation Order(s);

(3) the date and time of the transmission or indicating when the electronic evidence was made available to the recipient;

(4) information regarding the means of transmission (e.g. a record of the secure link through which the electronic evidence was made available, proof of receipt or delivery from postal services, etc. ([2]));

(5) the full file name(s) of the electronic evidence transmitted or otherwise made available to the intended recipient in the issuing State;

(6) the data size of the electronic evidence transmitted or otherwise made available to the intended recipient in the issuing State;

(7) at least one hash digest of the data which were transmitted or made available, and an indication of the hash algorithm(s) used. The hash algorithm(s) used for computing those hash digest(s) shall be a cryptographically strong one(s), in common use, and not subject to publicly disclosed weaknesses such as collisions (for example, SHA-512, SHA3-512, BLAKE2 or RIPEMD-160, but potentially a stronger one, depending on technological developments);

(b) where applicable, shall indicate as part of the manifest referred to in point (a) above the date and time until which the electronic evidence will remain accessible. This period shall provide the competent authority in the issuing State with a reasonable timeframe to retrieve the electronic evidence, which shall be no less than 10 calendar days and no more than 45 calendar days from the moment the electronic evidence is made available. At the request of the competent authority of the issuing State, the period indicated by the originator may be extended in an individual case;

(c) may record and transmit any additional information or remarks relevant to the case to the authority to which the electronic evidence has been transmitted or made available, as part of the manifest referred to in point (a) above.

3.4. Having regard to Article 28 of Regulation (EU) 2023/1543, the reference implementation software shall programmatically collect, transmit or otherwise provide access to the statistics referenced in paragraph 2 of that Article in both structured (e.g., XML) and unstructured (e.g., PDF) data formats. In accordance with Article 28(3) of Regulation (EU) 2023/1543, where technically equipped, national portals ([3]) operated by Member States may also transmit or provide these statistics to the Commission through an automated process. The Commission shall issue guidance on the data structure and the method for collecting and communicating these statistics.

([1]) For greater clarity, references to competent national authorities shall, *mutatis mutandis*, also be understood as applying to Eurojust national members, European Prosecutors, and European Delegated Prosecutors, insofar as they are empowered to perform the same functions under EU law and national law.

([2]) It should be recalled that in accordance with Article 19(5) transmission through such alternative means of communication shall meet the requirements of being swift, secure and reliable, allowing the recipient to establish authenticity.

([3]) 'National portals' should be understood as national 'IT systems' that form part of the decentralised IT system, as defined in Article 3(21) of Regulation (EU) 2023/1543.

4. **Communication protocols**

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

(a) communication within the decentralised IT system between competent authorities,

(b) communication within the decentralised IT system between competent authorities and Union agencies and bodies,

(c) communication between competent authorities and service providers through an API and the web-based interface, and

(d) communication with the Court database.

4.2. For the definition and the transmission of structured data and metadata, the components of the decentralised IT system shall be based on comprehensive and broadly accepted industry standards and protocols, such as SOAP and REST, notably those referenced by European standardisation organisations, such as ETSI.

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

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

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

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

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

4.5. Where applicable, the e-evidence XML Schemas shall make use of relevant standards or vocabularies, which are necessary for the proper validation of the elements and types defined within this schema. These may include:

(a) EU e-Justice Core Vocabulary;

(b) Unqualified Data Types;

(c) A code list for European Union Language Codes.

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

4.6. The Commission shall define the specifications for the common API, which shall be made available by enforcing States to service providers as a means of accessing the decentralised IT system. To the extent possible and reasonable, this API shall be based on ETSI TS 104 144 ('Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers').

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

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

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

(c) Public key infrastructure and Digital Signatures for secure key exchange and message integrity verification, using digital certificates (X.509) issued by trusted Certification Authorities (CAs).

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;

(b) measures to ensure the integrity of data (messages, forms, documents and electronic evidence) 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 availability by ensuring continuous access to services and data, preventing disruptions due to cyberattacks or failures;

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

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

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

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

5.4. 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 ([4]) and Directive (EU) 2016/680 of the European Parliament and of the Council ([5]), as applicable.

5.5. 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.

5.6. 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.

5.7. 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, for the IT systems under their responsibility that form part of the decentralised IT system.

6. **Electronic evidence** ([6]) **encryption**

6.1. Without prejudice to the security measures provided by the decentralised IT system, when issuing a European Production Order competent authorities may additionally supply a dedicated X.509 public certificate for asymmetric encryption of electronic evidence.

([4]) 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).

([5]) 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).

([6]) For the avoidance of doubt, the term 'electronic evidence' is confined to the definition provided in Article 3(8) of Regulation (EU) 2023/1543.

6.2. The issuance, management, verification, and all related aspects of the certificates referenced in point 6.1, along with the corresponding public key infrastructure, shall be the sole responsibility of the issuing State.

6.3. Without prejudice to future technological developments, the public certificates shall support industry-standard encryption algorithms such as, RSA (Rivest–Shamir–Adleman) or ECDH (Elliptic Curve Diffie-Hellman) for ECC (Elliptic Curve Cryptography).

6.4. Public certificates shall feature the appropriate 'keyUsage' extension, such as 'keyEncipherment' or 'dataEncipherment' for RSA-based certificates, and 'keyAgreement' for ECC-based certificates. Certificates shall be made available in PEM (Privacy-Enhanced Mail) or DER (Distinguished Encoding Rules) format.

6.5. Where the issuing authority has supplied an X.509 public certificate, and where a service provider sends the produced electronic evidence pursuant to a European Production Order, the provider shall, prior to the transmission of that data through the decentralised IT system, encrypt the electronic evidence using the respective X.509 public certificate supplied by the issuing State.

6.6. Where the issuing authority has supplied an X.509 public certificate, but where the transmission of electronic evidence in encrypted form is not possible due to technical or other justifiable reasons, and without prejudice to the provision under Article 19(5) of Regulation (EU) 2023/1543, the service provider may transmit the data without content encryption. In such cases, the service provider shall provide a reasoned explanation to the issuing authority.

7. **Minimum availability objectives**

7.1. Member States, Eurojust and the European Public Prosecutor's Office 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.

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

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

7.4. Member States, Eurojust and the European Public Prosecutor's Office 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.

7.5. Where Member States, Eurojust or the European Public Prosecutor's Office have fixed regular maintenance windows, they shall inform the Commission and the participants in the decentralised IT system of the time and day(s) when such fixed regular windows are planned. Notwithstanding the obligations set out in point 7.4, should components of the decentralised IT system under the responsibility of Member States, Eurojust or the European Public Prosecutor's Office become unavailable during such a regular fixed window, they may choose not to notify the Commission on each occasion.

7.6. In case of unexpected technical failure of the components of the decentralised IT system under the responsibility of Member States, Eurojust or the European Public Prosecutor's Office, they shall inform the Commission and the participants in the decentralised IT system about this failure without delay, and, if known, of the projected recovery timeframe.

7.7. In the event of maintenance activities or an unexpected technical failure of components within the decentralised IT system under a Member State's responsibility with adverse impact on the availability of the API and/or the web-based interface for service providers, the Member State concerned shall promptly make this information available on a website and/or communicate it to service providers operating within its territory, without undue delay.

7.8. In case of unexpected technical failure of the Court database, the Commission shall inform without delay the Member States, Eurojust and the European Public Prosecutor's Office of this unavailability, and if known, of the projected recovery timeframe.

7.9. In the event of a service disruption, Member States, Eurojust, and the European Public Prosecutor's Office shall ensure swift service recovery and minimal data loss, in accordance with the Recovery Time Objective and Recovery Point Objective.

7.10. Member States, Eurojust, and the European Public Prosecutor's Office shall implement appropriate measures to achieve the availability objectives outlined above and establish procedures for effectively responding to incidents.

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

8.1. Having regard to Article 19 of Regulation (EU) 2023/1543, for the purposes of the functioning of the decentralised IT system it is essential to establish an authoritative database on the service providers and competent authorities.

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

(a) for the purposes of Article 19 of Regulation (EU) 2023/1543, information on the competent authorities notified pursuant to Article 31(1)(a)-(c) thereof, including with regard to:

(1) Eurojust national members, together with an indication of whether they are authorised under national law to issue European Production Orders and European Preservation Orders in accordance with Article 8(3) and (4) of Regulation (EU) 2018/1727 of the European Parliament and of the Council ([7]);

(2) the European Delegated Prosecutors and European Prosecutors, where notified by Member States in accordance with Article 105(3) of Council Regulation (EU) 2017/1939 ([8]) as a competent issuing authority in the meaning of Regulation (EU) 2023/1543;

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

(c) information necessary for the correct functioning of and technical message routing of data exchanges within the decentralised IT system.

8.2.1. Information referred to in point 8.2(c) shall include the following:

(a) information on the Member State where the service provider's designated establishment is established or where its legal representative resides:

(1) Member State;

(2) central authority;

([7]) 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).

([8]) 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).

(b) information on service provider:

(1) name;

(2) address/Seat;

(3) registration number;

(4) legal form;

(5) phone number;

(6) email;

(c) information on designated establishment/legal representative:

(1) type of entity (Designated Establishment / Legal Representative);

(2) name;

(3) address/Seat;

(4) phone number;

(5) email;

(6) general contact person/entity;

(7) official language(s) accepted by the service provider / Designated Establishment / Legal Representative;

(8) services referred to in Article 2(1) of Directive (EU) 2023/1544 of the European Parliament and of the Council ([9]) offered in the Union;

(9) type of EU legal instruments for which the Designated Establishment / Legal Representative is designated (in situations where Member States do not take part in all the relevant EU legal instruments);

(10) territorial scope of designation/appointment;

(d) authentication of the information:

(1) name of authorised representative;

(2) job title;

(3) address;

(4) phone number;

(5) email;

(6) date.

8.2.2. Where available, information referred to in point 8.2(c) may include:

(a) information on service provider:

(1) contact person for queries on the notifications (if different from signatory);

(2) website;

(b) types of Data Available:

(1) for each Service Concerned:

— types of Data Available;

— category of Data;

— identifiers;

— period of Data Availability;

([9]) Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

(2) additional information on the data;

(3) additional information on the service (e.g. subcontracting relationships);

(c) information on designated establishment/legal representative:

(1) other service providers this designated establishment or legal representative is designated for;

(2) technical assistance contact information;

(3) emergency contact;

(d) technical information:

(1) name of technical contact point;

(2) phone number of the technical contact point;

(3) email of the technical contact point;

(4) API URL for dynamically retrieving information on the types of Data;

(5) connection type to national IT system:

— web-based interface;

— API;

— Push API URL.

8.3. In view of the operational needs of the decentralised IT system:

(a) the Commission shall be responsible for the development, maintenance, operation and support of the authoritative database;

(b) the Commission shall make access to the authoritative database possible via an API made available to the competent authorities, Eurojust and the European Public Prosecutor's Office for the purposes of their participation in the decentralised IT system;

(c) Member States shall ensure that the information on their competent authorities set out in points 8.2(a) and (b) in the authoritative database is complete, accurate and maintained up to date;

(d) the authoritative database shall enable Member States to provide and update the information on their service providers therein, and the authorities participating in the decentralised IT system to programmatically access and retrieve that information;

(e) Member States and service providers shall ensure that the information set out in point 8.2(c) in the authoritative database is complete, accurate and maintained up to date.