COMMISSION IMPLEMENTING REGULATION (EU) 2022/422

of 14 March 2022

laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1783 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) 2020/1783 of the European Parliament and of the Council of 25 November 2020 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (taking of evidence) ([1]), and in particular Article 25(1) thereof,

Whereas:

(1) In order to establish the decentralised IT system for communication and exchange of documents for the purposes of taking evidence, it is necessary to define and adopt technical specifications, measures and other requirements for the implementation of that system.

(2) There are tools that have been developed for the digital exchange of case related data, without replacing or requiring costly modifications to the existing IT systems already established in the Member States. The e-Justice Communication via On-line Data Exchange (e-CODEX) system is the main tool of this type developed to date.

(3) The decentralised IT system should be comprised of the back-end systems of Member States and interoperable access points, through which they are interconnected. The access points of the decentralised IT system should be based on e-CODEX.

(4) Once the decentralised IT system has been developed the steering committee will ensure the operation and maintenance of it. The steering committee should be established by the Commission in a separate act.

(5) 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 ([2]) and delivered an opinion on 24 January 2022.

(6) The measures provided for in this Regulation are in accordance with the opinion of the Committee on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters,

HAS ADOPTED THIS REGULATION:

Article 1

Technical specifications of the decentralised IT system

The technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Article 25 of Regulation (EU) 2020/1783 shall be as set out in the Annex.

([1]) OJ L 405, 2.12.2020, p. 1.

([2]) 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).

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, 14 March 2022.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

Technical specifications, measures and other requirements of the decentralised IT system referred to in Article 1

1. **Introduction**

The Taking of Evidence (ToE) exchange system is an e-CODEX based decentralised IT system that can carry out exchanges of documents and messages related to the taking of evidence between the different Member States in accordance with Regulation (EU) 2020/1783. The decentralised nature of the IT system would enable data exchanges exclusively between one Member State and another, without any of the Union institutions being involved in those exchanges.

2. **Definitions**

2.1. 'HyperText Transport Protocol Secure' or 'HTTPS' means encrypted communication and secure connection channels;

2.2. 'Portal' means the Reference Implementation solution or the National Back-end solution connected to the decentralised IT system;

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 digital signatures;

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 digital signatures;

2.5. '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;

2.6. '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;

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

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

The ToE exchange system shall use service-based methods of communication, such as Web-services or other reusable Digital Service Infrastructures for the purpose of exchanging messages and documents.

Specifically, it will use the e-CODEX infrastructure, which is comprised of two major components, the Connector and the Gateway.

The Connector is responsible for handling communication with the Reference Implementation solution or national implementations. It can process message exchange with the Gateway in both directions, trace messages and acknowledge them using standards such as ETSI-REM evidences, validate signatures of business documents, create a token that holds the outcome of the validation in PDF and XML format and create a container using standards such as ASIC-S where the business content of a message is packed and signed.

The Gateway is responsible for the exchange of messages and it is agnostic of the message content. It can send and receive messages to and from the Connector, validate header information, identify correct processing mode, sign and encrypt messages and transfer messages to other Gateways.

4. **Communication protocols**

The ToE exchange system shall use secure internet protocols, such as HTTPS for portal and decentralised IT system components communication and the standard communication protocols, such as SOAP, for the transmission of structured data and metadata.

Specifically, e-CODEX provides a strong information security by taking advantage of state of the art authentication and multilayer cryptographic protocol.

5. **Security standards**

For the communication and distribution of information via the ToE exchange 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 (HTTPS);

(b) measures to ensure the integrity of data while being exchanged;

(c) measures to ensure the non-repudiation of origin of the sender of information within ToE exchange 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;

(e) measures to ensure the authentication and authorisation of any registered users and measures to verify the identity of systems connected to the ToE exchange system;

(f) the ToE exchange system will be developed in accordance with the principle of data protection by design and by default.

6. **Availability of services**

6.1. The service time frame shall be 24 hours, 7 days a week, with a technical availability rate of the system of at least 98 % excluding scheduled maintenance.

6.2. Member States shall notify the Commission 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 of up to 12 hours;

(c) 30 working days in advance for maintenance operations, which may cause up to 6 days unavailability period per year.

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

6.4 Where Member States have fixed weekly service windows, they shall inform the Commission of the time and day of the week when such fixed weekly windows are planned. Without prejudice to the obligations set out in point 6.2, if Member States' systems become unavailable during such a fixed window, Member States may choose not to notify the Commission on each occasion.

6.5 In case of unexpected technical failure of the Member States' systems, Member States shall inform the Commission without delay of their system unavailability, and, if known, of the projected resuming of the service.

6.6 In case of unexpected failure of the database of Competent Authorities, the Commission shall inform the Member States without delay of the unavailability, and if known, of the projected resuming of the service.